ELECTRONIC HACKING AND SUBVERSION AS TOOLS OF FOREIGN POLICY: A NEOCLASSICAL REALIST ANALYSIS OF CYBER POWER

by

LAURENCE CAROMBA

Thesis submitted in fulfilment of the requirements for the degree

Doctor of Philosophy with specialisation in Political Science

(PhD Political Science)

in the

DEPARTMENT OF POLITICAL STUDIES AND GOVERNANCE

FACULTY OF THE HUMANITIES

UNIVERSITY OF THE FREE STATE

BLOEMFONTEIN

JUNE 2023

Study Leaders:

PROF HUSSEIN SOLOMON

PROF THEODOR NEETHLING

"One of the most effective forms of industrial or military sabotage limits itself to damage that can never be thoroughly proven – or even proven at all – to be anything deliberate. It is like an invisible political movement; perhaps it isn't there at all. If a bomb is wired to a car's ignition, then obviously there is an enemy; if a public building or a political headquarters is blown up, then there is a political enemy. But if an accident, or a series of accidents, occurs, if equipment merely fails to function, if it appears faulty, especially in a slow fashion, over a period of natural time, with numerous small failures and misfiring – then the victim, whether a person or a party or a country, can never marshal itself to defend itself."

- Philip K. Dick,
A Scanner Darkly

"What has shaken me is not that you lied to me, but that I no longer believe you."

- Friedrich Nietzsche,
Beyond Good and Evil

Acknowledgements

I would like to express my profound appreciation to everyone who provided the support and assistance that was necessary for the completion of this thesis. A special note of gratitude goes to my research supervisors, Prof. Hussein Solomon and Prof. Theodor Neethling. Their constant encouragement, perceptive advice, and patience were invaluable throughout this project – especially during the challenging years of the Covid-19 pandemic when progress was often slow and difficult. I am extremely fortunate to have been guided by supervisors who were generous with their extensive knowledge and deep insights into International Relations, while also granting me the freedom to follow my interests and explore unconventional ideas.

I extend my sincere appreciation to my colleagues: Prof. Victoria Graham, Prof. Heidi Brooks, Prof. Susan Booysen, Prof. Anna-Mart van Wyk, Dr. Yacoob Abba Omar, Terry Shakinovsky, Prof. Susan Graham, Dr. Fay Hodza, Dr. Reza Hosseini, and all the other outstanding researchers and professionals I have had the privilege of working with while carrying out research on this project. Their friendship, encouragement, and intellectual engagement have significantly contributed to my academic growth. I also wish to convey my gratitude to my friend and colleague, Chiara Santi Laurini. Her willingness to accommodate my numerous requests for feedback and engage in thoughtful discussions about this project have been invaluable. I would also like to extend my thanks to Joan Hettema, whose diligent proofreading and valuable input have greatly enhanced the quality and clarity of this work.

I am deeply indebted to my parents, who introduced me to the complex world of politics at a young age and sparked my enduring interest in this fascinating academic discipline. Their nurturing of my intellectual growth and their unconditional love have been pivotal to the success of this project.

Finally, I would like to express my immense gratitude to Kylie, whose unfaltering support and relentless encouragement were indispensable in my journey to complete this project. Thank you.

Abstract

This study develops a new theory of cyber power as a tool of foreign policy, focusing on sovereign states as the unit of analysis and drawing from the theoretical assumptions that are inherent in the realist paradigm of International Relations. This theory describes and classifies the nature of cyber power in international politics, and seeks to explain why different states make differing choices about which cyber strategy to adopt.

The study introduces a conceptualisation of cyber power that incorporates both computer hacking and social media disinformation campaigns within a single framework, in which both types of cyber operations are understood as methods for degrading and destroying trust. It then analyses the utility, limitations, and costs associated with technical and persuasive of cyber power, and argues that both forms require the attacking state to accept significant trade-offs. This suggests that states are unlikely to use these tools unless they have pressing reasons to do so. Building upon on this insight, the study then develops a new typology of four cyber strategies: “restrained”, “technical-aggressive”, “persuasive-aggressive”, and “combined-aggressive”. It hypothesises that cyber strategy selection by states is primarily determined by two independent variables: their external security requirements and their institutional preferences. States with high external security requirements are more likely to make aggressive use of technical cyber power, while states with negative institutional preferences are more likely to make aggressive use of persuasive cyber power. This theory provides a parsimonious and compelling explanation for cyber strategy selection.

To test and apply the theory, three empirical case studies are conducted on Brazil, the United States of America, and the Russian Federation. The findings reveal that Brazil has adopted a restrained strategy, while the United States has chosen a technical-aggressive strategy, and Russia has selected a combined-aggressive strategy. These empirical findings are congruent with the expectations of the theory.

Lastly, the theory is applied to predict how the cyber strategies of these states might evolve if their associated independent variables were to change. The resulting analysis suggests that the emergence of multipolarity in the international system is likely to be associated with the increased use of both technical and persuasive cyber power by state actors.

Table of Contents

Table of Figures ..... **ix**

List of Abbreviations ..... **x**

APT Codenames Used in this Study ..... **xiii**

Notes on Terminology ..... **xiv**

Chapter 1 Introduction: Cyber Power as a Tool of Foreign Policy **1**

1.1 Introduction 1

1.2 Research Question 3

1.3 Thesis Statement: A Theory of Cyber Power 4

1.4 Definition of Key Concepts 5

1.4.1 Cyber Space and the Cyber Domain 5

1.4.2 Cyber Power and Security 6

1.4.3 Types of Cyber Operations 7

14.4 Cyber Strategies 9

1.5 Technical Terminology 10

1.5.1 Advanced Persistent Threats 10

1.5.2 Distributed Denial-of-Service 11

1.5.3 Technical Exploits 11

1.5.4 Social Engineering 13

1.5.5 Social Media 14

1.6 Theoretical Assumptions 15

1.6.1 Assumption #1: States Can Be Modelled as Unitary Actors 16

1.6.2 Assumption #2: States Can Be Modelled as Self-Interested Security Seekers 18

1.6.3 Assumption #3: States Create Institutions to Advance Their Interests 20

1.6.4 Assumption #4: We Can Make Probabilistic Predictions About State Behaviour 22

1.7 Research Methodology 23

1.7.1 Meta-Theoretical Position: Soft Positivism 24

1.7.2 Research Design: Case Study Approach 27

1.7.3 Case Selection Criteria: Control, Variation, and Testability 29

1.7.4 Data Collection Method: Triangulation of Qualitative Data 31

1.7.5 Data Analysis Method: Congruence Testing and Cross-Case Comparison 35
1.8 Chapter Outline 36
Chapter 2 Literature Review: The Quest for a Theory of Cyber Politics 38
2.1 Introduction 38
2.2 Transnationalism: New Actors and Interactions 40
2.2.1 Arquilla & Ronfeldt: Transnationalism & Networks 43
2.2.2 Rosecrance, Keohane, and Nye: The Liberal Transnationalists 45
2.2.3 Choucri: Lateral Pressure in Cyber Space 47
2.2.4 Kello: Transnationalism and Transformation 50
2.3 Constructivism: Norms and Securitisation in Cyber Space 52
2.3.1 The Cyber Securisation Theorists 54
2.3.2 Valeriano and Maness: Cyber Regionalism & Restraint 56
2.4 Realism: Bringing the State Back In 58
2.4.1 Clarke & Knake: Cyber War and National Security 60
2.4.2 Rid, Lindsay, and Gartzke: The Sceptical Realists 62
2.4.3 Segal and Klimburg: Strategic Culture in Cyber Space 64
2.4.4 Buchanan: The Cyber Security Dilemma 66
2.5 Other Perspectives 68
2.6 Conclusion 69
Chapter 3 Theorising Cyber Power and Cyber Strategies 72
3.1 Introduction 72
3.2 Technical and Persuasive Cyber Power 74
3.3 The Attribution Problem 77
3.4 Features of Technical Cyber Power 81
3.4.1 Its Destructive Potential is Unknown 82
3.4.2 It Is Coercively Weak 85
3.4.3 It Undermines Trust in Technical Systems 90
3.4.4 The Trade-Offs of Technical Cyber Power 93
3.5 Features of Persuasive Cyber Power 96
3.5.1 It Operates Within a Broader Information Market 96
3.5.2 It Exploits Homophily and Memetic Transmission 100
3.5.3 It Undermines Trust in Institutions 104
3.5.1 The Trade-Offs of Persuasive Cyber Power 107

3.6 Explaining Cyber Strategy Selection 109
3.6.1 External Security Requirements 111
3.6.2 Institutional Preferences 113
3.7 Four Ideal-Type Cyber Strategies 115
3.8 Conclusion 117
Chapter 4 Brazil 120
4.1 Introduction 120
4.2 Brazil's Restrained Use of Technical Cyber Power 121
4.2.1 Building Up Potential Technical Cyber Capability 121
4.2.2 Refraining from Using Its Offensive Capabilities 127
4.3 Brazil's Restrained Approach to Persuasive Cyber Power 129
4.3.1 Internet Governance and Soft Power 130
4.3.2 Maintaining Trust in the Brazilian Information Market 132
4.4 Brazil's Restrained Strategy 136
4.5 Explanatory Variables 137
4.5.1 Low External Security Pressures 140
4.5.2 Positive Institutional Preferences 144
4.6 Conclusion 147
Chapter 5 The United States 149
5.1 Introduction 149
5.2 The United States' Aggressive Use of Technical Cyber Power 150
5.2.1 Waging the War on Terror 151
5.2.2 Opposing Nuclear Proliferation 155
5.2.3 Engaging in Great Power Rivalry 159
5.3 The United States' Restrained Approach to Persuasive Cyber Power 161
5.3.1 The Internet Freedom Agenda 162
5.3.2 Public Diplomacy 168
5.3.3 Maintaining Trust in the American Information Market 171
5.4 The United States' Technical-Aggressive Strategy 173
5.4.1 Cyber Security Trade-Offs 174
5.4.2 Commercial Trade-Offs 177
5.4.3 Balancing and Retaliation 179
5.5 Explanatory Variables 180

5.5.1 High External Security Requirements 183
5.5.2 Positive Institutional Preferences 186
5.6 Conclusion 190
Chapter 6 Russia 192
6.1 Introduction 192
6.2 Russia's Use of Technical Cyber Power 193
6.2.1 Preserving Influence in the Baltics and the Caucasus 194
6.2.2 Destabilising Ukraine 199
6.2.3 Engaging in Great Power Rivalry 205
6.2.4 Cyber Arms Control 207
6.3 Russia's Use of Persuasive Cyber Power 210
6.3.1 Amplifying Divisions in the United States 210
6.3.2 Intervention in United States Presidential Politics 216
6.3.3 Dividing the European Union 221
6.3.4 Insulating Russia's Information Market 224
6.4 Russia's Combined-Aggressive Strategy 226
6.4.1 Commercial Trade-offs 228
6.4.2 Trade-Offs to Social Cohesion 229
6.4.3 Balancing and Retaliation 230
6.5 Explanatory Variables 232
6.5.1 External Security Pressures 235
6.5.2 Institutional Preferences 240
6.6 Conclusion 244
Chapter 7 Conclusion: The Future of Cyber Power 247
7.1 Introduction 247
7.2 Limitations of the Findings 248
7.3 Main Findings 249
7.3.1 Brazil: The Restrained Strategy 251
7.3.2 The United States: The Technical-Aggressive Strategy 252
7.3.3 Russia: The Combined-Aggressive Strategy 254
7.4 Predictions that Flow from this Theory 257
7.4.1 Scenario #1: Hegemonic Brazil 257
7.4.2 Scenario #2: Brazil Under Siege 259

7.4.3 Scenario #3: Revisionist United States 260
7.4.4. Scenario #4: Neo-Isolationist United States 262
7.4.5. Scenario #5: Status Quo Russia 263
7.4.6 Scenario #6: A World of Parallel Institutions 265
7.5 Contribution to the Field 267
7.6 Avenues for Future Research 269
7.7 Conclusion 270
Bibliography 273

Table of Figures

Figure 1: A visual summary of the main thesis of this study. 4
Figure 2: Summary of the major schools of thought identified in this chapter. 40
Figure 3: Summary of the most important authors discussed in this chapter. 70
Figure 4: Comparison of classification systems for cyber operations. 77
Figure 5: A typology of four ideal-type cyber strategies. 116
Figure 6: Brazil's location within the typology of cyber strategies. 137
Figure 7: The United States' location within the typology of cyber strategies. 173
Figure 8: Russia's location within the typology of cyber strategies. 227
Figure 9: Summary of the overall findings of this study. 256
Figure 10: Summary of possible cyber strategy scenarios 266

List of Abbreviations

ABIN	Brazilian Intelligence Agency
AIIB	Asian Infrastructure Investment Bank
AIVD	General Intelligence and Security Service
APT	Advanced Persistent Threat
BBG	Broadcasting Board of Governors
BRI	Belt and Road Initiative
BRICS	Brazil, Russia, India, China, and South Africa
CCSDCiber	Cybersecurity and Defence Coordination Centre
CDCiber	Cyber Defence Centre
CEPESC	Centre for Research and Development of Secure Communications
CFR	Council on Foreign Relations
CGI.br	Internet Steering Committee
CIA	Central Intelligence Agency
CNA	Computer Network Attack
CNE	Computer Network Exploitation
ComDCiber	Cyber Defence Command
COMECON	Council for Mutual Economic Aid
CSCC	Centre for Strategic Counterterrorism Communications
CSIRT	Computer Security Incident Response Team
CSIS	Centre for Strategic and International Studies
CSTO	Collective Security Treaty Organisation
DARPA	Defence Advanced Research Projects Agency
DCCC	Democratic Congressional Campaign Committee
DDoS	Distributed Denial-of-Service
DNC	Democratic National Committee
DSIC-GSI	Department of Information and Communication Security
EAEU	Eurasian Economic Union
ENaDCiber	National School of Cyber Defence
EU	European Union
FBI	Federal Bureau of Investigation
FOC	Freedom Online Coalition
FSB	Federal Security Service

FTAA	Free Trade Area of the Americas
GATT	General Agreement on Tariffs and Trade
GCHQ	Government Communications Headquarters
GDPR	General Data Protection Regulation
GIFT	Global Internet Freedom Task Force
GRU	Main Intelligence Directorate
GSI	Institutional Security Bureau
IANA	Internet Assigned Numbers Authority
IBSA	India, Brazil, South Africa
IDF	Israel Defence Forces
ICANN	Internet Corporation for Assigned Names and Numbers
IMF	International Monetary Fund
IP	Internet Protocol
IRA	Internet Research Agency
IS	Islamic State (also known as ISIS or ISIL)
IT	Information Technology
ITU	International Telecommunication Union
JCDD	Joint Cyber Defence Detachment
JCPOA	Joint Comprehensive Plan of Action
MERCOSUR	Southern Common Market
NAFTA	North American Free Trade Agreement
NATO	North Atlantic Treaty Organisation
NDB	New Development Bank
NGO	Non-Governmental Organisation
NHS	National Health Service
NIC.br	Network Information Centre
NOBUS	“Nobody But Us”
NSA	National Security Agency
ONR	Office of Naval Research
OTF	Open Technology Fund
PNSI	National Information Security Policy
PROSUR	Forum for the Progress and Development of South America
RT-RG	Real Time Regional Gateway
SCO	Shanghai Cooperation Organisation

SIGINT	Signals Intelligence
SVR	Foreign Intelligence Service
TAO	Tailored Access Operations
TPP	Trans-Pacific Partnership
UK	United Kingdom
UNASUR	Union of South American Nations
URCC	Unit for Combating Cybercrime
USA	United States of America
USAGM	United States Agency for Global Media
USSR	Union of Soviet Socialist Republics
VEP	Vulnerabilities Equities Process
WTO	World Trade Organisation

APT Codenames Used in this Study

Name of APT	Suspected Agency	Suspected State Sponsor
“Comment Crew”	PLA	People’s Republic of China
“Cozy Bear”	SVR	Russian Federation
“Equation Group”	NSA	United States of America
“Fancy Bear”	GRU	Russian Federation
“Lazarus Group”	Unknown	North Korea
“Sandworm”	GRU	Russian Federation
“Shadow Brokers”	Unknown	Possible connection with Russia

Notes on Terminology

This study uses the upper-case term “International Relations” to refer to the academic discipline that studies international politics. It uses the lower-case phrase “international relations” to refer to the pattern of relations between states which is the primary object of study in that discipline.

To maintain linguistic consistency, this study uses the term “cyber” as a freestanding prefix (for example, “cyber power” or “cyber security”) except when referring to specific agencies or documents that employ this terminology differently.

Chapter 1
Introduction: Cyber Power as a Tool of Foreign Policy

1.1 Introduction

In July 2016, WikiLeaks, a website that publishes material from anonymous sources, released a searchable database of 19,252 emails that had been stolen from the servers of the United States Democratic National Committee (DNC) (WikiLeaks, 2016). The emails were released three days before the Democratic National Convention, and contained embarrassing revelations about the Committee's favouritism toward Hillary Clinton, who would eventually become the Democratic nominee for president (Hamburger & Tumulty, 2016). These revelations caused outrage among supporters of Clinton's left-wing rival, Bernie Sanders, and frustrated Clinton's attempts to unite her party after a divisive primary contest. Four months later, Clinton lost the presidential election, with poor Democratic turnout in the key states of Pennsylvania, Michigan, and Wisconsin proving to be the decisive factor in her loss.

This incident was an example of a growing phenomenon in international politics: a state-sponsored cyber operation. It was carried out by a group of Russian hackers who operated under the pseudonym "Guccifer 2.0" (Mueller, 2019, pp. 45-48). The Russian hackers used a combination of deceptive emails and malicious software to gain access to the DNC's computer network and steal large numbers of emails, which they then handed over to WikiLeaks. According to a consensus report by US intelligence agencies (DNI, 2017), which was reinforced by subsequent reports by Robert Mueller (2019) and the United States Senate (2019), Russia's primary goal with this operation was to swing the election in favour of Clinton's opponent in the presidential election, the Republican candidate Donald Trump.

During the first three years of the Trump Administration, much of the American political class was obsessed with the various Russian cyber operations that had occurred in the run-up to the 2016 election. Why, they wondered, did the Russian government seem to support Trump? Had the Trump campaign knowingly colluded with the Russian government? Was Trump, in effect, an agent of the Russian state? These questions formed the background to Mueller's investigation, which Trump repeatedly branded a "witch hunt", and which ultimately failed to produce answers that satisfied either side.

However, there is another question, lurking in the background, that few Americans thought to ask: why was Russia the *only* state that used cyber power to interfere in the US election?

After all, the United States is a large and influential country whose policies significantly impact other nations. During Trump's presidency, the US underwent several important policy shifts in its diplomatic and trade relations: it became more protectionist, less friendly toward Europe, more hostile toward Iran, friendlier toward Israel and Saudi Arabia, more conciliatory toward North Korea, and less interested in tackling the problem of climate change. Regardless of whether one agrees or disagrees with these policies, it is undeniable that they created both winners and losers in other regions of the world. Why, then, did countries that might have benefited from a Trump victory not join Russia in conducting cyber campaigns to support his candidacy? And why did states that might have benefited from a Clinton victory not counteract these efforts with their own cyber campaigns in support of her candidacy?

We might also ask why the United States does not appear to conduct subversive cyber operations similar to the ones that Russia carried out during the 2016 US election? Why does the United States not launch a cyber campaign in France, for instance, with the aim of increasing the likelihood that pro-American French politicians will win elections, or to increase French support for the North Atlantic Treaty Organisation (NATO)? It seems certain that the United States could carry out such operations if it wished to. It possesses extremely high levels of cyber capability. It has used these capabilities to carry out intrusive espionage and even launch physically destructive cyber attacks against other countries. And yet, the United States seems strangely reluctant to engage in online subversion of the sort that Russia has conducted.

These questions are specific instances of a broader theoretical puzzle that informs this study: the observed discrepancy between the cyber strategies of different states. This dissertation seeks to answer these questions, thus contributing to the growing body of literature that has investigated computer hacking and electronic propaganda in international politics. Scholarly interest in these issues has increased since 2008 due to increasingly high-profile cyber operations by states. However, despite substantial scholarly interest in these issues, there are significant gaps in the existing literature. Firstly, the subfield has not adequately integrated the study of "hard" forms of cyber power, such as distributed denial-of-service (DDoS) attacks or hacking of critical infrastructure, with "soft" forms of cyber power such as persuasion, propaganda, and subversion. Secondly, much of the existing research has been descriptive rather than explanatory. It describes the capabilities and

effects of cyber operations, helping us understand what these tools are capable of. However, there has not been a sustained theoretical effort to explain the variation among states' cyber strategies. This study aims to fill this gap. It examines the use of cyber operations as tools of foreign policy and asks why some countries have made intensive use of these tools while others have not. It offers an explanation that is grounded in the scholarly theories of International Relations, particularly realism. It offers an integrated understanding of both the hard and soft forms of cyber power – referred to in this study as "technical" and "persuasive" cyber power, respectively – and develops a novel framework that treats both forms of cyber power as methods for attacking trust. Furthermore, this study also examines the trade-offs of cyber power, as well as the gains associated with using these forms of cyber power. It argues that cyber power is not cost-free, and that its use requires states to accept certain painful trade-offs. These trade-offs include possible economic harms, reduction in domestic trust, and the possibility of triggering balancing behaviour or retaliation by other states.

This study uses these insights to develop a novel typology of cyber strategies, and argues that states will tend to select one of these strategies based on their external security requirements and their institutional preferences. This theory helps to explain why Russia carried out its cyber operations in support of Trump, as well as similar operations supporting nationalist candidates in France and other countries. It suggests that these operations were motivated by Russia's perceived insecurity and its desire to weaken trust in international institutions such as NATO and the European Union (EU). If this theory is valid, it would not only explain Russia's cyber strategy – it would also provide a general explanation for cyber strategy selection that can be applied to other states.

1.2 Research Question

This study seeks to answer the following two research questions:

1. What are the distinct features of cyber power as a tool of foreign policy, and what are the possible strategies that states can adopt to take advantage of cyber power?
2. What are the factors and variables that influence a state's choice of cyber strategy, and how can these be integrated into a theoretical framework to explain and predict which cyber strategies a particular state will adopt?

By understanding the key features of cyber power, and the variables that explain a state's choice of cyber strategy, we can explain why states make the strategic choices they do – and make contingent

predictions about how state cyber strategies are likely to evolve if their circumstances were to change.

1.3 Thesis Statement: A Theory of Cyber Power

This study argues that cyber power can be conceptually divided into two sub-types: "technical cyber power" and "persuasive cyber power." Technical cyber power aims to undermine trust in networks and technical systems, while persuasive cyber power seeks to erode trust in epistemic authorities and political institutions. However, both types of cyber power generate significant costs and trade-offs for states that employ them. Consequently, states will only make use of these tools if they have important goals that they wish to accomplish, and they believe that the payoffs from achieving these goals will outweigh the associated costs.

		External Security Requirements	
		Low	High
Institutional Preferences	Positive	Restrained use of technical cyber power Restrained use of persuasive cyber power	Aggressive use of technical cyber power Restrained use of persuasive cyber power
	Negative	Restrained use of technical cyber power Aggressive use of persuasive cyber power	Aggressive use of technical cyber power Aggressive use of persuasive cyber power

Figure 1: A visual summary of the main thesis of this study.

The main hypothesis of this study is that there are two main variables that influence this choice. The first variable is the level of external security requirements that the state faces. States with high external security pressures typically have a combination of expansive foreign interests that require defence, geographic vulnerability, powerful and threatening rival states within their region, and ongoing territorial disputes. Conversely, states with low security pressures tend to possess less ambitious foreign policy goals, have defensible geographic borders, lack powerful and hostile

regional rivals, and are not engaged in ongoing conflicts. Thus, the first hypothesis of this study is that states facing high security pressures will adopt more aggressive technical cyber operations.

The second variable in this framework is the state's institutional preference. States tend to create institutional frameworks to advance their interests when they are in a position of strength. Over time, some states benefit from these institutions, leading to positive institutional preferences, while others feel they would benefit more from a different set of institutions, resulting in negative institutional preferences. States with negative institutional preferences aim to sow distrust in existing institutions, leading to their breakdown. Thus, the second hypothesis of this study is that states with negative institutional preferences will employ more aggressive persuasive cyber operations.

In summary, this study argues that the most crucial determinant of a state's cyber strategy is not the personality of its leader, its ideology, its domestic regime type, its strategic culture, or even its technical capability. Instead, it advances the idea that we can explain and predict the most important tendencies of a state's cyber strategy using a relatively parsimonious framework consisting of just two distinct variables: the severity of the state's external security requirements, and its preference for strengthening or weakening international institutions. Once we understand a state's security pressures and its institutional preferences, we can effectively explain and predict the cyber strategy it will adopt.

1.4 Definition of Key Concepts

There are a number of key concepts and terms that are used in this study, which must be defined in order to ensure conceptual clarity. Many of these are concepts that were originally developed in other contexts, such as computer science or even science fiction, and were later adopted by policymakers and political scientists. These terms are not always used consistently across various academic and professional fields, which can sometimes result in confusion. As such, it is necessary to specify how these terms will be used in this study.

1.4.1 Cyber Space and the Cyber Domain

This study is concerned with the ways in which states pursue their foreign policy interests within the context of global electronic communication networks, a context that is sometimes referred to as "*cyberspace*" or "*the cyber domain*". The use of the term "cyberspace" to refer to digital networks

originated with the science fiction author William Gibson (1984) in his book *Neuromancer*, which anticipated the development of an interconnected global communications network. During the early 1990s, the word "cyberspace" was sometimes used interchangeably with "the internet". Over time, however, this usage has fallen out of fashion, and the prefix "cyber" has instead become more strongly associated with the issue of computer security. Some authors are critical of this trend, arguing that the word "cyber" has become a catch-all term that is too vague to be analytically useful (Shires & Smeets, 2017). However, as Segal (2016) notes, the term has become entrenched within government, military, intelligence, and foreign policy circles; and so, whatever its analytical strengths or weaknesses are, we are stuck with it.

When using the term "cyber space", this study adopts the definition offered by Segal (2016): "the global network of interconnected information technologies and the information on it". This definition encompasses all the information contained on the public internet as well as private computer networks; intranets disconnected from the global internet; the so-called "deep web" and "dark web";[1] and the physical layer of hardware on which the internet runs. However, this definition only includes technology; it does not include the human beings who use the internet or the social systems they create.

On the contrary, this study uses the term "cyber domain" to refer to a broader concept that includes the hardware and software layers of the Internet, as well as the human social systems that are layered on top of it (Kello, 2017, p. 45) This concept is frequently used in government and military circles, although some technologists dislike the term and prefer to avoid it (Segal, 2016). The term 'cyber domain' sometimes carries militarised connotations, suggesting that cyberspace has become a domain of warfare – along with the conventional domains of land, sea, and air – within which military force may legitimately be employed (Aucsmith, 2012; Hayden, 2011, p. 4). However, it is conceptually useful to have a term that encompasses both the technological and social dimensions of global information technologies, and it is in this sense that the concept will be used in this study.

1.4.2 Cyber Power and Security

A core concept used in this study is "*cyber power*". Several scholars in the field of International Relations have previously defined this concept. For example, Nye (2010, pp. 3-4) defines cyber

[1] The "deep web" consists of websites that are not accessible from public search engines. The "dark web" is a portion of the deep web that is protected by encryption and is sometimes used for illegal activities.

power as “the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain”. Valeriano and Maness (2015, p. 28) define it as “the ability to apply typical forms of control and domination in [cyber space]”. Although these definitions are helpful, they lack the detail needed for our purposes. As such, Chapter Three of this study focuses on conceptualising and unpacking the nature of cyber power as a tool of foreign policy, describing its capabilities and its inherent limitations.

The basic definition of cyber power used in this study is as follows: it is a state’s capacity to influence or alter the behaviour of actors beyond its borders by manipulating computer networks, and to avoid being influenced by other actors through the manipulation of its own computer networks. This definition is restrictive, in the sense that it situates the concept within the context of international relations and limits our focus to sovereign states. However, it is also broad, encompassing both technical aspects, such as the ability to exploit vulnerabilities in digital infrastructure, and persuasive aspects, including the use of information operations that shape the perceptions and actions of targeted audiences. In essence, this definition treats cyber power as a resource used by states to advance their interests in the international system, employing a diverse range of tactics and strategies to achieve their desired outcomes in the cyber domain.

A related concept is “*cyber security*”. Hundreds of definitions for this term are used by scholars and government agencies worldwide, but this study follows the definition used by the International Telecommunications Union (ITU), which defines cyber security as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user’s assets” (ITU, 2009). Compared to the concept of cyber power discussed earlier, this definition of cyber security is much narrower. The definition of cyber power used in this study is fundamentally political in its orientation, whereas the definition of cyber security is more technical. Furthermore, while the definition of cyber power focuses on both offensive and defensive capabilities, the definition of cyber security is largely defensive and focused on the practices used to secure software, computers, and networks.

1.4.3 Types of Cyber Operations

States exercise their cyber power by carrying out various actions in the cyber domain. To avoid confusion, it is helpful to establish a typology of these actions.

This study uses the term "*cyber operation"* to refer to a specific, organised, and purposeful action conducted by a state in the cyber domain. This term describes a broad category of events: cyber operations can be offensive or defensive, and can vary greatly in terms of their impact on the adversary and their level of technical sophistication. Cyber operations are used to achieve a variety of goals, including gathering intelligence, disrupting information systems, stealing sensitive data, or influencing the behaviour of targeted audiences. They often involve a combination of technical exploits and social engineering tactics; terms that are discussed in more detail in Section 1.5 of this chapter.

The term "*cyber attack*" is used in this study to describe a specific type of cyber operation that is designed to inflict pain on an adversary. This definition purposefully excludes pure intelligence-gathering operations, which are generally designed to be undetected. By contrast, cyber attacks are noticeable, and are usually carried out in service of a broader strategy of coercion or compellence. The most common forms of cyber attack attempt to inflict harm on an adversary by disrupting their electronic systems or destroying electronic data. However, there are certain rare examples of cyber attacks that go one step further and cause destruction in the physical world, analogous to what might be achieved by a conventional weapon. Notable examples of physically destructive cyber attacks include the Stuxnet attack against Iran in 2009, which destroyed some of its enrichment centrifuges, and two cyber attacks against Ukraine's electricity grid and power plants in 2015 and 2016, both of which led to power outages.

A "*cyber campaign*" is a series of cyber operations conducted in succession, with the aim of achieving a specific political goal. Similarly, a "*cyber conflict*" is a sustained or intense confrontation between states in the cyber domain, which could involve multiple cyber campaigns aimed at achieving complementary objectives. Cyber conflicts often take place alongside other forms of international conflict, such as the use of economic sanctions or warfare. Furthermore, since cyber operations often tend to provoke retaliation, a cyber conflict will often develop into a multi-sided competition in which there are at least two sides carrying out cyber campaigns against each other.

Lastly, the term "*cyber war*" is used in this study to refer to a hypothetical extreme form of cyber conflict, in which two sides try to coerce each other using cyber attacks that have the potential to cause injury, destruction, or death in the physical world. This definition is informed by the writings of Rid (2013, p. 37), who argues that "[a]n act of war must be instrumental, political, and potentially lethal, whether in cyberspace or not". This is a deliberately restrictive definition, reflecting the

inherently violent nature of war. By this definition, to date, there has never been a true cyber war. The events that come closest are, arguably, the aforementioned power grid hacks and the subsequent NotPetya cyber attack against Ukraine in 2016. These cyber operations had the potential to cause deaths, although there is no evidence that they actually did so (Greenberg, 2019, pp. 200-203). A clearer example of a cyber war – albeit, one that never left the planning stages – was "Nitro Zeus", a leaked plan for a US cyber campaign against Iran that would have disabled power plants, communications networks, and air defences (Sanger & Mazzetti, 2016).

14.4 Cyber Strategies

Finally, a core concept used in this study is that of a "*cyber strategy*". For the purposes of this study, a cyber strategy can be defined as a pattern of behaviour in the cyber domain that is aimed at achieving specific interests while navigating the trade-offs between competing priorities.

There are two important elements in this definition that require further elaboration. First, a cyber strategy is defined as a pattern of behaviour, rather than a written document or a "master plan". This understanding of strategy draws inspiration from Luttwak's (2009, p. 409) analysis of the grand strategy of the Byzantine Empire, in which strategy is defined as "the level at which knowledge and persuasion, or in modern terms intelligence and diplomacy, interact with military strength to determine outcomes in a world of other states". According to Silove (2018), this definition implies that a national strategy need not be written down, or even be intentional. Written documents are useful to understand a state's self-conception of its own strategy, but the document is not the strategy. Instead, according to Silove (2018, p. 43), "grand strategy refers to a pattern of behaviour… [t]he pattern *is itself the grand strategy*" (Silove, 2018, p. 43, emphasis in original). Taking this argument one step further, Luttwak (2009, p. 409) observes that "all states have a grand strategy, whether they know it or not". Applying this logic to the cyber domain, we might observe that all states – after crossing the technological threshold that enables them to make use of cyber power – also have a cyber strategy, whether they know it or not.

A second aspect of this definition of cyber strategy used in this study is that it calls attention to the close conceptual relationship between strategy and trade-offs. The very notion of "strategy" both presupposes and requires the existence of actors who have to make trade-offs between competing interests and priorities. This point is captured succinctly by Porter (1996, p. 70) in a famous quote on business strategy: "The essence of strategy is choosing what not to do. Without trade-offs, there

would be no need for choice and thus no need for strategy." Chapter 3 of this study demonstrates that all forms of cyber power require states to make trade-offs.

1.5 Technical Terminology

In addition to the conceptual terms mentioned above, this study also employs various technical terms from the fields of cyber security and computer science. While these terms are generally not contested, they are specialised, and it is useful to define them for the benefit of readers who may not be familiar with these fields.

1.5.1 Advanced Persistent Threats

"Advanced Persistent Threats" (APTs) are malicious actors that are widely considered to be the most dangerous and capable hacking groups on the internet. They target specific organisations for prolonged periods of time, using a combination of technical exploits and social engineering to penetrate networks and exfiltrate data (Singer & Friedman, 2014, pp. 55-60). They are distinguished from other cyber criminals by their use of sophisticated technical methods, the targeted nature of their attacks, and their apparent selection of targets according to political rather than purely economic criteria (Kaspersky, 2019).

It is widely believed that most APTs are secretly controlled by states, although few states will openly take credit for an APT operation. In a meta-analysis of APT attribution by four private cyber security firms, 127 of 170 identified APTs were attributed to states (Romanosky & Boudreaux, 2019, p. 8). Most of the public information on APTs comes from private cyber security firms that focus on countering their activities, such as FireEye, CrowdStrike, and Kaspersky Labs. These firms typically track APTs over time by identifying similarities between their operations and periodically release research reports announcing the discovery of new APTs. It should be noted that private cyber security firms have commercial incentives and are not dispassionate researchers; however, they possess a high level of technical expertise and are generally well-regarded in the field of computer security.

Examples of well-known APTs include the Chinese group "Comment Crew," the Russian APTs "Fancy Bear" and "Sandworm," and the US-based "Equation Group." Since APTs operate covertly, they do not have official names, and so they are generally referred to using codenames assigned by security companies. However, each firm maintains its own database of APTs and follows different

conventions for naming them, which can result in considerable confusion (Romanosky & Boudreaux, 2019, pp. 9-10). For example, the Russian APT "Fancy Bear" (a codename created by CrowdStrike) is also known as APT28 (by Mandiant), Sofacy Group (by Kaspersky) and STRONTIUM (by Microsoft). In general, this study refers to APTs using the names for which they are most famous. For example, the name "Fancy Bear" was widely used in media coverage of Russian interference in the 2016 US presidential election, so this study uses the term Fancy Bear to describe this group. However, the reader should be aware that APTs might be named differently in other sources.

1.5.2 Distributed Denial-of-Service

"Distributed denial-of-service" (DDoS) attacks are a simple class of cyber operation in which a website or online service is deliberately overwhelmed with traffic, blocking access for legitimate users. These attacks are relatively easy to organise, requiring only a coordinated network of compromised computers (or "*bots"*). However, they do not cause lasting damage and typically result in only temporary inconvenience for the victim.

DDoS attacks were famously used by Russian hackers against Estonia in 2007 and Georgia in 2008, initially sparking significant interest in their potential as a foreign policy tool. Russell (2014) compared the attacks to a naval blockade, and NATO (2014) even suggested that future DDoS operations might trigger the collective security provision of the North Atlantic Treaty. However, the DDoS operation against Estonia yielded no policy concessions, and governments rapidly learned to defend their networks against such cyber operations (Valeriano & Maness, 2015, p. 145). In the subsequent decade, few states engaged in DDoS attacks. In 2017, US Cyber Command carried out a DDoS attack against North Korea in retaliation for previous provocations, but this was widely regarded as an ineffective and symbolic response (DeYoung, Nakashima, & Rauhala, 2017; Gallagher, 2017).

1.5.3 Technical Exploits

In contrast to DDoS operations, which only block access to a service, "*technical exploits"* take advantage of vulnerabilities that grant unauthorised access to systems and networks to intruders. A "*vulnerability"*, in the context of computer security, is a flaw in the design of computer software, hardware, or networks that could potentially allow the creation of an exploit. Thousands of vulnerabilities in popular software packages are discovered each year, although only a small percentage of these lead to the creation of practical exploits.

Vulnerabilities exist because modern software is extremely complex, and no human-created system is ever perfectly secure. As such, all major software vendors have adopted a continuous security model in which they update previously-shipped software and patch new vulnerabilities as they are discovered. This leads to an endless arms race, with defenders trying to identify and patch vulnerabilities, and attackers attempting to exploit them before they can be patched. Although it is theoretically possible that we might someday reach a point where all software vulnerabilities have been discovered and fixed, in practice, commercial incentives drive software companies to release new versions, inadvertently creating new vulnerabilities in the process.

Exploits can be categorised into two broad types: *"known exploits"* and "*zero-day exploits"*. Known exploits take advantage of vulnerabilities that have already been discovered and documented, which makes these exploits less likely to succeed. However, they can still be very damaging. Software vendors may be slow to patch vulnerabilities, and users might not bother applying software updates and security patches once they are available. In 2017, for example, the British National Healthcare Service (NHS) suffered financial damages equivalent to £92 million after its IT managers neglected to update its systems and it was attacked using a previously known vulnerability (Department of Health and Social Care, 2018, p. 14).

Zero-day exploits, on the contrary, take advantage of vulnerabilities that are unknown to software developers. The name "zero-day" refers to the fact that the vendor has had zero-days of warning when the exploit is first used. Since the underlying vulnerabilities that are exploited by zero-days are, by definition, unpatched, these exploits are very likely to succeed and are highly prized by state actors and criminal hackers alike. However, once a zero-day exploit is used, it is typically quickly discovered and patched, which means that it is no longer a zero-day. Thus, a zero-day exploit is an unusual weapon that is effectively destroyed upon use.

Exploits are used to create malicious software, or "*malware"*: software that causes harm to the user or the computer running it. Common examples of malware include viruses, which spread by attaching themselves to other files; trojans, which are disguised as legitimate software; worms, a dangerous class of malware that spreads without user intervention; ransomware, which encrypts victims' data and demands payment in order to access it; and logic bombs, which are designed to remain dormant until activated by a predetermined condition.[2] There are persistent rumours that

[2] For a useful discussion of different forms of malware, written for non-specialists, see Singer & Friedman (2014).

some states have already prepared the battlefield for future cyber wars by implanting stealthy logic bombs within the communications, command-and-control, and civilian infrastructure systems of potential adversaries, although it is difficult to confirm whether this is true.

1.5.4 Social Engineering

Even in cases where no technical exploits exist, APTs and other hackers still have ways to gain unauthorised access to computers and networks. It is a truism of cyber security that human beings constitute the weakest link in any sufficiently complex system (Libicki, Ablon, & Webb, 2015, p. 33). The use of deception or psychological manipulation to trick users into divulging confidential information is known as "*social engineering"* and it is one of the oldest and most reliable methods used by computer hackers.

The most common social engineering attacks are "*phishing"* scams, in which the attacker sends a message to the victim over email or some other communications platform and poses as a legitimate institution in order to steal the victim's credentials or passwords. Phishing scams have a low rate of success, so they typically rely on mass targeting and self-selection by victims. As such, this method is not especially useful for APTs and other actors who wish to carry out targeted cyber operations against a particular individual or organisation.

"Spear phishing" is a more sophisticated version of phishing in which the message is tailored to be persuasive to a particular recipient. Attackers generally begin a spear phishing campaign by researching their victim using social media platforms, which can enable them to gather extensive information and dramatically increase their likelihood of success (Salahdine & Kaabouch, 2019, p. 5; Wilcox, Bhattacharya, & Islam, 2014). Although targeted spear phishing operations demand significantly more time and effort than traditional phishing scams, they are very difficult to counter and are a favourite tactic among APTs (FireEye, 2016, p. 4; Proofpoint, 2018, p. 17). Symantec (2019, p. 51) estimates that 65% of APT intrusions use spear phishing as the initial entry method, rather than zero-days or other technical exploits.

Another type of social engineering method involves the use of an insider threat. An insider threat is a member of an organisation who exploits their privileged position to facilitate sabotage or espionage against the organisation. Malicious insiders may be motivated by financial, ideological, or personal goals, while non-malicious insiders might cause harm due to carelessness. The act of recruiting an insider threat blurs the boundary between cyber operations and traditional spycraft.

1.5.5 Social Media

"*Social media*" platforms such as Facebook, Twitter, and Instagram enable users to create, share, and engage with content. These allow users to create online communities and have become primary news sources for many demographics. They are generally designed to encourage high levels of interaction, content sharing, and user attention. Some psychologists worry about the addictive properties of these technologies.[3] The typical use pattern for social media applications is eerily similar to the "variable interval reinforcement" method of psychological control used in the experiments of B. F. Skinner (1965). The user posts content online and is rewarded with affirmation from other users, stimulating dopamine activity in the brain – but this reward is doled out inconsistently, creating a feedback loop of posting and validation-seeking (Haynes, 2018). In Skinner's (1965, p. 102) experiments, such inconsistent rewards were found to be a powerful method of behavioural conditioning.

Due to the enormous volume of information that passes through them, social networks have become far too large for humans to effectively curate or moderate. As a result, technology companies have come to rely heavily on "*algorithmic targeting"* to automatically classify and recommend content. Through statistical inferences drawn from other users, companies can make fairly accurate predictions about the type of content their users will enjoy. This technology allows companies such as Facebook to take posts from hundreds of sources and combine them into a manageable newsfeed (World Wide Web Foundation, 2018, pp. 4-5). However, malicious actors can sometimes find ways to game the system and manipulate algorithmic content recommendation algorithms, in order to artificially increase the size of their audience.

One side-effect of algorithmic content recommendation is the creation of *"filter bubbles*". This describes a situation in which algorithmic recommendation becomes a self-fulfilling prophecy. A user might click on a piece of content, perhaps by chance, and then be exposed to a cascade of follow-up content that amplifies and reinforces the original message. If the user continues to click on these new recommendations, the algorithm will feed them more extreme versions of the same basic theme, while increasingly filtering out opposing views (Pariser, 2011, pp. 9-10). This has the potential to result in the radicalisation of individuals who make use of algorithmic services as their primary method for learning about the news.

[3] See Cocoradă, Maican, Cazan, and Maican (2018); Salehan and Negahban (2013). Some psychologists have drawn a connection between smartphone over-use and depression, especially in younger users; see Twenge, Joiner, Rogers, and Martin (2017), and Whillans and Chen (2018).

A related dynamic is the creation of online "*echo chambers"*. Social media users tend to cluster together with other users who hold similar views, forming online communities in which they predominantly interact with other users who hold similar biases and prejudices. Within these spaces, users tend to reinforce each other's beliefs, and contrary views are excluded. This differs from the filter bubble phenomenon described above in the sense that filter bubbles are caused by algorithmic recommendation, whereas echo chambers are caused by voluntary self-sorting of users. However, they result in similar problems: they prevent users from being exposed to competing views and result in increased radicalisation and polarisation. The implications of these social dynamics are discussed in Chapter Three.

Social media platforms facilitate the rapid spread of information, making them an attractive vector for actors seeking to manipulate public opinion. "*Disinformation campaigns*" (which are sometimes referred to as "*fake news"*) are cyber operations designed to spread false or misleading information through social media platforms. Disinformation campaigns involve the deliberate creation and dislargeemination of false or misleading information to deceive and manipulate public opinion. Social media platforms provide a fertile environment for such campaigns due to their wide reach and the relative weakness of truth-selecting dynamics on these networks (discussed in Chapter Three). Malicious actors make use of various tools to carry out such campaigns, including automated accounts (*"bots"*), human-operated accounts (*"trolls"*), and fictitious personas (*"sockpuppets"*). Bots are automated accounts that can be programmed to perform specific tasks, such as posting content or interacting with other users. Trolls, on the other hand, are human-operated accounts that engage in deceptive or provocative behaviour to elicit emotional reactions and sow discord. Sockpuppets are false online personas created by malicious actors to infiltrate online communities and manipulate discussions.

Having defined the key concepts and terminology relevant to this study, we now consider theoretical assumptions and methodological processes that are used in this study.

1.6 Theoretical Assumptions

To construct a theory of cyber power, this study makes several simplifying assumptions about the nature of states and the international system. It assumes that we can learn something useful about states by modelling them as unitary actors; that states can be treated as self-interested security seekers; that states create institutions to promote their interests; and that it is possible for researchers to make contingent and probabilistic predictions about state behaviour. These

theoretical assumptions primarily stem from the realist paradigm of International Relations, which is associated with authors such as Waltz (1979). However, several of these assumptions are also compatible with other theoretical paradigms, such as institutionalism and constructivism. The following sections will consider each of these assumptions in more detail.

1.6.1 Assumption #1: States Can Be Modelled as Unitary Actors

Firstly, this study makes the methodological assumption that we can gain meaningful insight into the foreign policies and cyber strategies of states by modelling them as unitary actors. A unitary actor refers to the idea that a state's decisions and actions can be treated as though they are a single, unified entity. As such, sovereign states are treated as the basic units of analysis in this study, rather than sub-state actors such as individual leaders, factions, interest groups, political parties, or government bureaucracies. Many influential scholars in International Relations have adopted this state-centric approach, including Waltz (1979), Keohane (1984), Fearon (1995), and Wendt (1999). The unitary actor model is employed here as a methodological tool, rather than a literal depiction of reality. Nevertheless, the unitary actor model has several advantages that make it suitable for this particular study.

By modelling states as unitary actors, it becomes possible to simplify the analysis of any given state, which allows us to develop more parsimonious explanations for its strategy than would otherwise be the case (Lake, 2008). States are complex entities with numerous internal actors, competing interests, and institutional processes that shape their foreign policy decisions. By bracketing this internal complexity and treating states as singular entities, researchers can identify general patterns and trends that would otherwise be lost in the chaos. Rather than focusing on the minutiae of the bureaucratic processes of each state, we can identify overarching variables guiding states across time and administrations. Furthermore, this approach allows for structured and focused comparison between states in a way that facilitates theory development. By focusing on state-level variables, we can identify common factors that are applicable to multiple states – for example, their level of power within the international system. These large-scale patterns and variables would be obscured if attention were primarily focused on the internal dynamics within each state.

This assumption of a unitary actor is, of course, an abstraction. States are, obviously, not unitary actors in a literal sense. It is therefore important to acknowledge the limitations of modelling states as unitary actors: this approach may not fully capture the nuances and complexities of state behaviour, particularly when internal dynamics play a significant role in shaping foreign policy

decisions. However, by abstracting away from the complexities of internal politics, this approach enables scholars to develop generalisable theories and hypotheses that can explain and predict state behaviour across different contexts and historical periods. This approach suggests that even though states are not really unitary actors, we can learn something useful by treating them as such.

At once, an important question arises: does it make sense to construct a theory of cyber politics that is focused on states? Some authors, such as Kello (2017, p. 165) argue that it does not: "The cyber domain does not tolerate [state-centric] theoretical preconceptions." There are indeed many capable non-state actors in the cyber domain.[4] However, a careful reading of the historical record suggests that a state-centric methodological bet is indeed a valid approach to the study of cyber politics. There are simply no empirical examples of cyber operations by non-state actors that have been able to match the political impact or technical sophistication of cyber operations carried out by states. Non-state actors do engage in cyber operations – but they are unable to match the vast financial resources, human capital, persistence, and long-term planning horizons of states.

Consider the resources that were required to carry out the Stuxnet cyber attack, which is discussed in more detail in Chapter Five of this study. Stuxnet made use of four Windows zero-day vulnerabilities, which would be prohibitively expensive for a non-state actor to acquire (Zetter, 2014a). Furthermore, Stuxnet was also part of a larger covert operations programme against Iran, which was funded with a budget of US$ 300 million and used the assets of established intelligence agencies such as the Central Intelligence Agency (CIA), the NSA, and Mossad (J. R. Lindsay, 2013, p. 288). These agencies combined their resources to map the Iranian network, recruit insider threats within Iran, and penetrate the Iranian "air gap".[5] The attackers even constructed a fully functional mock-up of the Iranian centrifuge cascade, in order to test and debug the malware before it was launched (Langner, 2013, p. 20). This is far beyond the capability of any non-state actor.

Furthermore, states possess a range of legislative and regulatory powers that are not available to any non-state actor. These powers ultimately stem from the monopoly on coercive force that states enjoy within their territories, and their control over the physical infrastructure layer of the internet

[4] See Bussolati (2015) and Sigholm (2016) for more discussion of this general issue. Many of the most famous non-state actors in the cyber domain are politically motivated "hacktivist" collectives, such as Anonymous, WikiLeaks, and LulzSec. However, criminal actors motivated by pure economic interests are much more common (McGuire, 2018).

[5] An air gapped network is a network that is physically separated from the internet. In theory, this is an effective form of computer network defence; however, to be useful, a computer network must have some mechanism for updating software or exporting data, creating potential entry points for attackers.

(Nye, 2010, p. 9). States can engage in escalation dominance: if they are unhappy with outcomes in the cyber domain, they can escalate conflicts into the domain of physical violence (Singer & Friedman, 2014, p. 152). Liberal democratic states do not usually use the full range of these powers, but this reflects a legal and political choice rather than an intrinsic limitation of state actors on the internet. Other states have made different choices. For example, the People's Republic of China, through a combination of content regulation and industrial policy, has created an "alternate internet" in which users are served by Chinese technology companies and regulated according to Chinese rules (K.-F. Lee, 2018, p. 71). For all these reasons, sovereign states are exceptional actors in the cyber domain, and it is reasonable to try to construct a theory that focuses on explaining and understanding their actions.

1.6.2 Assumption #2: States Can Be Modelled as Self-Interested Security Seekers

Secondly, this study assumes that states predominantly act as self-interested security seekers, with their choice of cyber strategy reflecting a cost-benefit analysis in terms of security outcomes. The assumption that states can be treated as self-interested security seekers is associated with the realist paradigm in International Relations, which assumes that states will adopt strategies to enhance their power and ensure their survival. This assumption underpins the works of prominent realist scholars such as Waltz (1979), Morgenthau (1993), and Mearsheimer (2003), who emphasise the tendency of states to prioritise their security in an environment characterised by uncertainty and potential threats. The assumption that states can be modelled as self-interested actors also informs the broader rationalist paradigm, which draws insights from game theory and neoclassical economics, and includes scholars such as Keohane (1984) and Fearon (1995).

This view assumes that states can be understood to have "national interests", which are interests that apply to the overall state and can be used to make inferences about its behaviour. The concept of national interest is widely used in popular, official and scholarly discourses on international relations, although it remains a controversial and contested concept in International Relations.[6] For analytical purposes, this study proceeds according to the abstract assumption that states have certain preferences that are held by the state as a collective entity rather than by individuals or groups within it. These preferences are pursued on behalf of (although often without the explicit endorsement or approval of) the entire population, and remain relatively constant over time.

[6] See discussion by Morgenthau (1949), Krasner (1978), E. H. Carr (2016) and Lake (2008). For critical perspectives on the national interest, see arguments by Wendt (1992), Trubowitz (1998), Chomsky (1981), and Cox (1981).

One clear example of a preference that meets the above criteria is “survival”, which is often seen as the archetypal example of a national interest in International Relations. Waltz (1979, p. 105) argues that states’ intrinsic interest in survival effectively compels them to engage in self-interested and security-seeking behaviour: since the international system is anarchic and has no overarching authority to enforce order, each state is forced to follow a policy of self-help and build up military forces to deter potential aggressors (Waltz, 1979, p. 105). However, this in turn creates systemic insecurity and the potential for conflict, incentivising states to continually seek out opportunities to balance against other states which become too powerful (Waltz, 1979, p. 164). States which do not adopt this balancing strategy are eliminated from the international system, and other states learn from these failures (Waltz, 1979, p. 195). Over time, this has the effect of reducing unit variation in the international system, encouraging all states to adopt similar security-focused strategies regardless of their domestic regime type or preferred ideology (Waltz, 1979, p. 97).

Although it is most clearly identified with realism and rationalism, the assumption that states are self-interested security seekers is also compatible with non-rationalist theoretical paradigms such as constructivism. For instance, while realists typically argue that security-seeking behaviour is conditioned by the anarchic nature of the international system, constructivists such as Wendt (1999) maintain that states engage in such behaviour because they are influenced by conflict-generating norms and beliefs within the international system. Regardless of whether this assumption is rooted in a realist or constructivist ontology, treating states as self-interested security seekers provides a powerful explanatory framework for understanding the foreign policies and strategies of states within the international system. It allows for the development of generalisable theories and hypotheses that can explain and predict state behaviour across various contexts and historical periods. While this approach does not capture all the nuances of state behaviour, the treatment of states as self-interested security seekers has been an enduring method for studying the dynamics of international relations, and it offers useful insight into a state’s selection of its cyber strategy.

In some of the previous research on cyber power, conceptions of the state interests in the cyber domain have tended to be incomplete or underspecified. Valeriano and Maness (2015), in keeping with their broader constructivist epistemology, are sceptical of the concept of objective national interests in the cyber domain. Instead, they argue that aggressive behaviour in the cyber domain is more often motivated by “rivalry”, which they define as the social process by which states are assigned the role of the enemy (Valeriano & Maness, 2015, p. 52). They suggest that rivalrous behaviour is often motivated less by rational strategic calculations and more by a “simple, and

perhaps immature, position of denying a gain to the enemy" (Valeriano & Maness, 2015, p. 52). Rivalrous states are described as "addicted to perpetual conflict", and willing to "cut off the nose to spite the face" (Valeriano & Maness, 2015, p. 52). However, this explanation is unsatisfactory. While it is true that conflict behaviour is inevitably accompanied by a hardening of attitudes toward the other party (Galtung, 1996, p. 72; Mitchell, 1989, p. 71), rivalry does not account for the full range of state strategies in the cyber domain, and risks overlooking the strategic benefits that they may wish to achieve by engaging in cyber conflict.

Other scholars assume that states do have objective national interests in the cyber domain. Buchanan (2017a, p. 23) points out that states have a national interest in collecting high-quality intelligence: this allows them to avoid strategic surprise, plan for threats and opportunities, and engage in more efficient bargaining. At the same time, states are also threatened by the intelligence collection efforts of their adversaries (Buchanan, 2017a, p. 24). Segal (2016) proposes a broader set of interests that he believes are consistent across the international system. According to Segal, all states wish to stimulate economic growth, protect their information assets, exploit and sometimes damage other countries' information assets, and gain access to their citizens' data for intelligence and law enforcement purposes (Segal, 2016, p. 42). By integrating economic and security interests, this perspective more closely captures the full range of state interests in the cyber domain. In addition, this study further assumes that states have an interest in maintaining trust and confidence in international institutions they rely on to advance their interest – or conversely, an interest in undermining trust in institutions that are antithetical to their interests.

1.6.3 Assumption #3: States Create Institutions to Advance Their Interests

A third assumption of this study is that states create and participate in international institutions to advance their interests. International institutions can be defined as formal or informal agreements, organisations, and sets of norms that lead to a convergence of expectations between states (Krasner, 1982, p. 185). These institutions define the "rules of the game" for state behaviour, providing a framework for cooperation, communication, and conflict resolution on a range of global issues. Institutions aim to ensure more stable and predictable patterns of competition in international relations and regulate the ways in which states pursue their interests.

The neo-liberal institutionalist theory in International Relations argues that states create institutions to overcome collective action problems. In this view, the international system is seen as analogous to a prisoner's dilemma, in which shared distrust and fear of defection prevent states from engaging

in mutually beneficial cooperation (Keohane, 1984). Institutions help to solve this prisoner's dilemma by increasing the level of information available to states, discouraging cheating, creating opportunities for iterated bargaining, and lowering the transaction costs associated with forming international agreements (Keohane, 1982, 1984). By establishing a predictable set of rules and fostering a shared expectation that promises will be adhered to, institutions allow states to address a range of practical problems – particularly in areas such as international trade, security, and environmental protection, where there is potential for positive-sum bargains that leave all participants better off.

However, realists such as Krasner (1991) and Mearsheimer (1994) argue that international institutions do not remove the incentives for conflict in the international system. Even if bargaining between states produces positive-sum gains, states are likely to disagree over how the resulting surplus should be divided. Furthermore, due to the inherent potential for conflict in the context of international anarchy, states have good reason to worry about relative gains, in addition to absolute gains. After all, if a bargain produces relative gains for one state that are much higher than for other states in the bargain, there is a possibility that the advantaged state might invest its gains in military force and then seize the entire surplus by force. Therefore, the design of international institutions is influenced by the zero-sum logic of politics as well as the positive-sum logic of economics, and international institutions tend to reflect the interests of the dominant states that created them.

This study integrates both realist and institutionalist insights on institutions. It assumes that international institutions do facilitate positive-sum bargaining, while also reflecting the interests of dominant states during their formation. The framework suggests that powerful states create and shape international institutions during periods in which their level of relative power is high. This helps them to maintain their dominance and secure interests over the long term, ensuring their continued advantage in international bargaining processes even if their relative power were to decline (Gruber, 2000; Kindleberger, 1981; Krasner, 1985). The result is that these states tend to obtain a disproportionately higher share of the surplus gains that result from positive-sum bargains. Perhaps the best-known example of this dynamic is the UN Security Council, which accords a privileged position to the main winners of the Second World War. This has resulted in an unusual situation where the United Kingdom – a middle-ranking power today – continues to hold permanent membership on the Security Council, while India, the world's most populous state, does not.

When states are confronted with an institutional order they perceive as unfair or stacked against them, they have several policy options in response. They might try to increase their level of influence in existing institutions or create new institutions that better suit their needs and interests. Alternatively, a state might attempt to undermine and weaken the existing institutions it finds unfavourable. Presumably, most dissatisfied states will pursue a combination of these policies, and attempt to strike a balance between creating alternative institutions and weakening institutions that do not serve their interests. However, Chapter Three of this study argues that the phenomenon of persuasive cyber power presents states with a stark choice about which of these two options it wishes to prioritise.

1.6.4 Assumption #4: We Can Make Probabilistic Predictions About State Behaviour

Lastly, this study assumes that it is possible to discern patterns and regularities in state behaviour and make probabilistic predictions about their future actions. This study aims to classify the range of cyber power strategies available to states and identify the state-level variables that explain why specific states choose the strategies they choose. Since it aspires to the goal of explanation, it necessarily assumes that causal patterns exist in international politics, and that it is possible to identify these patterns and make valid inferences about why events occur. Central to this study is the assumption that state behaviour, while complex and multifaceted, still follows discernible patterns that allow for probabilistic predictions about future actions.

Much of the seminal scholarship in International Relations aspires to identify the variables that influence state behaviour, and develop predictive models based on those variables. These encompass both "grand theories", as proposed by scholars like Keohane (1984), Mearsheimer (2003), and Waltz (1979), as well as "middle-range" theories such as the theory of democratic peace. Critically, these theories are inherently probabilistic rather than deterministic. Their predictions, devoid of claims to absolute certainty, furnish estimates on the probability of particular outcomes or state behaviours, all grounded in empirical evidence and theoretical premises. Ripsman, Taliaferro, & Lobell (2016, p. 107) elucidate this notion by stating:

> [T]he theories we develop and test in international relations are probabilistic theories… [P]robabilistic theory seeks to explain as much of the [dependent variable's] variance as possible with the [independent variables] and [intervening variables] it identifies but does not claim to explain 100 percent of that variance. Therefore, it posits that the theory should hold ceteris paribus but that other factors not enumerated in the theory

> may also affect outcomes. In this regard, democratic peace theory does not posit that liberal democracies will never wage war against other liberal democracies, just that, all things being equal, pairs of democracies should be far less likely to wage war against each other than any other dyad. (Ripsman *et al.*, 2016, p. 107)

The probabilistic approach to explanation used in this study draws inspiration from the logic of Bayesian inference, which emphasises the importance of updating prior assessments about causal mechanisms in light of new evidence from repeated observations (Bennett, Charman & Fairfield, 2022, pp. 5-7). Starting with initial assumptions about state behaviours in the realm of cyber strategies, this study makes a series of observation about each case that serve as an opportunity to update and refine these beliefs. This iterative research process, as advocated by scholars such as Bennett (2008) and Fairfield & Charman (2022), aims to whittle down the likelihood of opposing explanations being true. However, this assessment will never reach zero.

There are difficulties with this approach, however. As Ripsman et al. (2016, p. 107) point out, probabilistic theories are difficult to falsify, which reduces our confidence in their being true. However, while probabilistic logic introduces an element of ambiguity into the study of International Relations, it is necessitated by the genuine complexity and sensitivity that exists in the international political system. Overall, the probabilistic nature of this study is consistent with a broader meta-theoretical position grounded in "soft positivism", which is discussed in Section 1.7.1 below.

1.7 Research Methodology

The previous sections outline the theoretical assumptions that underpin this study. In general, this study operates according to the premise that states can be usefully modelled as self-interested actors that employ cyber power to advance their interests. It focuses on states as the primary unit of analysis and treats their cyber strategies as the dependent variable that requires explanation. The objective is to develop a theoretical framework that explains why states choose specific strategies over others and make contingent predictions about how their strategic choices might evolve if their geopolitical circumstances change. The following section discusses the research methodology used to achieve this goal.

This study follows a research process that begins with the deductive development of a theory and concludes with empirical analysis. It starts with the theoretical assumptions discussed in Section 1.6 of this chapter, which are primarily drawn from a "soft positivist" meta-theoretical position as well

as the broader realist paradigm in International Relations. Through the analysis of the technical features of cyber operations and a process of deductive logic, it hypothesises that there is a relationship between a given state's external security requirements and its institutional preferences, and the cyber strategy it will likely adopt. To test these hypotheses, this study examines a set of three cases, which are characterised by variation along the dependent variable.

Data is collected on each case using multiple sources, including investigative journalism, commercial threat intelligence reports, research reports by think tanks and government agencies, various datasets and data aggregators, and scholarly research. This research is used to develop a profile of each state's cyber strategy, as well as its external security requirements and institutional preferences. During the data analysis phase, two main methods are employed: the congruence method and cross-case analysis. The congruence method is used to assess the degree to which the empirical data collected for each case conforms to the expectations of the theory. In addition, cross-case analysis between the cases is used to identify consistent patterns and provide additional support for the validity of the theory. Based on this analysis, this study concludes that external security requirements and institutional preferences indeed play a significant role in shaping a country's choice of cyber strategy. Finally, a set of predictions is derived from this theory, demonstrating its utility for predicting future unforeseen events.

The following sections discuss the underlying philosophical and practical reasons for employing these methodological choices, including soft positivist meta-theoretical position, the reasons for selecting the case study approach, the criteria used for case study selection, the challenges associated with data collection in this area, and the analysis methods used to interpret the collected data.

1.7.1 Meta-Theoretical Position: Soft Positivism

This study is grounded in a meta-theoretical stance of "soft positivism". Soft positivism is a middle-ground approach between strict positivism and interpretivism. It recognizes that social reality is constructed and subjective but believes that patterns and regularities can still be discerned. This approach offers a nuanced perspective on the complexities inherent in the study of human behaviour, making it well-suited for International Relations.

Soft positivism acknowledges the complex and subjective nature of human social behaviour. However, it posits that human social systems, including the behaviour of collective entities like

states, operate according to discernible patterns – even if these are understood imperfectly (Bennett, 2004; Ripsman *et al.*, 2016, p. 105). Soft positivists recognise that while natural phenomena can often be predicted with a high degree of certainty, the behaviour of human beings – and by extension, the behaviour of collective social entities such as states – is complex and contingent. However, this does not necessitate a retreat into radical subjectivism. By employing rigorous methods like case studies and quantitative analysis, soft positivism believes that researchers can identify certain regularities in human social structures. This enables research to make inferences and probabilistic predictions about behaviour, although these causal inferences will always be incomplete and imperfect.

This soft positivist meta-theoretical position is consistent with the Bayesian or probabilistic approach to explanation described in Section 1.6.4. Methodologically, soft positivists see value in both quantitative and qualitative research methods, as offering multiple possible paths to understanding reality. While this position does not claim to offer deterministic certainties, it provides a range of probable outcomes based on accumulated evidence, prior beliefs, and observed patterns.

Ontologically, soft positivism argues objective reality exists, but acknowledges that our understanding of it is mediated through our perceptions and the concepts we use to define reality. In this sense, the soft positivist position can be understood as orthogonal to the broader debate between realism and anti-realism in the philosophy of science. Scientific realism assumes that theories provide a true representation of the world, even when discussing objects or processes that can not be directly observed. By contrast, anti-realists, argue that the value of theories lies in their predictive power, not necessarily their truth. In International Relations, scholars like Mearsheimer and Walt explicitly describe themselves as scientific realists, asserting that their goal is to develop theories that reflect the actual underlying realities of international politics (Mearsheimer & Walt, 2013, pp. 432-434). By contrast, a theorist such as Waltz (1979) is focused on developing parsimonious theories with explanatory power, and can therefore be understood as leaning towards scientific non-realism.[7]

To illustrate this ontological divide, it is useful to consider the classic statement of non-realism in the social sciences: Milton Friedman's (1953) argument that theories should be evaluated according to

[7] It should be noted that "realism" in the context of the philosophy of science has no relation with the realist paradigm of international relations. Some realist IR theorists are also realists in the former sense, but others are not.

the accuracy of their predictions, rather than the realism of their assumptions. This "instrumentalist" approach is controversial, and is not the approach that is employed in this study. And yet, Friedman's essay contains an important insight: realism can not be the only criterion used to judge the strength of a theory. In International Relations, concepts such as "states", "interests", "norms", "power", and "institutions" are foundational to the discipline, and yet these concepts are inherently non-realistic: they resist easy definition, and can not be measured using scientific instruments. Nevertheless, scholars continue to use these concepts because they are useful. A science of International Relations that did not make use of simplifying constructs would be too detailed to be useful; it would be like the 1:1 scale map imagined in Jorge Luis Borges' short story, *On Exactitude in Science*.

As discussed in Section 1.6, the research design of this study incorporates two assumptions that are explicitly non-realistic. The unitary state assumption, described in Section 1.6.1, deliberately abstracts the reality of interest group competition within the state, but it also facilitates the identification and cross-case comparison of state-level cyber strategies. The rational actor assumption, described in Section 1.6.2, is similarly non-realistic, but it is useful for generating consistent expectations about the behaviour of actors in the cyber domain which can then be compared to the historical record. Despite the use of these non-realistic concepts and assumptions, this study is broadly aligned with the realist philosophy of science. The two key variables identified in this study – external security pressures and institutional preference – are not treated as mere predictive tools, but are instead understood to be real concerns and drivers of policy. If the theory outlined in this study is valid, and if we could listen in on the cabinet meetings and strategy discussions of various states, we should expect to find evidence that foreign policy executives and other decision-makers genuinely do consider these variables when planning their cyber strategies.

Overall, soft positivism recognises the limitations and subjectivity of social science theorising and is cognisant of the roles of uncertainty, chance, and human agency in shaping international politics. Furthermore, it recognises that causal inferences in a field such as International Relations will always be imperfect and incomplete. However, soft positivists recognise that systematic efforts to understand causal mechanisms can nevertheless still be useful. Through careful analysis of cases and data, such research allows us to develop a rigorous and nuanced understanding of cause and effect in international politics, thereby enabling more informed decision-making in the realm of foreign policy. Furthermore, while this study makes use of several simplifying concepts, such as unitary

states, it assumes that the underlying causal mechanisms it identifies are real. The following sections discuss the research strategy that is employed to identify those causal mechanisms.

1.7.2 Research Design: Case Study Approach

The study uses the case study approach, a qualitative research methodology that involves an in-depth examination of a subject or phenomenon within its real-life context. Yin (2011, p. 3) defines a case study as an "empirical inquiry about a contemporary phenomenon (e.g., a 'case'), set within its real-world context." A key characteristic that sets case study research apart from atheoretical description is its use of specific cases to understand larger phenomena. Instead of merely describing individual events, case study research delves into the complexities of a particular instance to draw insights that can be applied to answer broader questions. As described by George and Bennett (2005, p. 5), a case study is "the detailed examination of an aspect of a historical episode to develop or test historical explanations that may be generalisable to other events." In this study, the focus is on three particular states and their cyber strategies. The goal is not only to understand these specific cases, but also to gain insight into cyber power and cyber strategies as general phenomena.

This study combines a case study approach with a broadly positivist meta-theoretical orientation, focusing on explanation and causal inference. Positivist research aims to identify patterns, relationships, and causal mechanisms that can be generalised beyond the specific cases under investigation. By employing a case study approach within a positivist framework, the study seeks to uncover the underlying factors that shape the use of cyber power in state foreign policy, as well as the potential causal relationships that may exist between state-level variables and cyber strategies. The combination of case study methods and a positivist orientation is a common research strategy in the field of International Relations, particularly for studies that aspire to explain the causes of international political phenomena (Bennett, 2004, p. 19; Odell, 2004, pp. 56, 66).

There are several reasons why this study opts for a qualitative approach instead of a quantitative one. The number of states in the world is limited, and the subset of states that possess the capability to incorporate cyber power into their foreign policy is even smaller. Furthermore, states, their cyber strategies, and the variables used to explain them are complex and multifaceted. This study incorporates variables such as a state's level of aggression in its use of technical and persuasive cyber operations, its security requirements, and its institutional preferences. These variables would be difficult to operationalise into simple numerical values that could be used for quantitative

hypothesis testing. While not impossible, doing so would likely require the development of new indices to accurately measure these concepts.

On the contrary, case study research has several advantages that make it well-suited to the research question in this study. Case studies allow for a large number of observations to be carried out within each case, as well as comparisons between cases (King, Keohane, & Verba, 1994, p. 225). Through qualitative examination of a smaller number of cases, it is possible to conduct rich and in-depth analyses to better understand the nuances and intricacies of each particular case. For this reason, Bennett and Elman (2007, p. 171) argue that case study methods have a comparative advantage in studying the "complex and relatively unstructured and infrequent phenomena that lie at the heart of the [International Relations] subfield".

With their focus on in-depth analysis, case study methods offer strong advantages in studying causality (George & Bennett, 2005, pp. 19-22). Although quantitative research typically relies on large datasets and statistical analysis to measure associations between variables, this approach may not provide a complete understanding of the causal processes at play. In contrast, case study research allows the researcher to delve deeper into individual cases and observe the operation of causal pathways and factors that might not be evident through quantitative analysis. This makes case study research well-suited for research that pursues soft positivist meta-theoretical goals.

It is important to recognise that case study methods also have certain weaknesses. Case studies are vulnerable to the problem of selection bias, whereby researchers unintentionally choose cases that confirm their preconceived notions or hypotheses. Although these dangers exist with other research methodologies, the risk is increased in case study research due to the smaller number of cases (Bennett, 2004, pp. 27-28). Furthermore, qualitative data can be subjective and open to interpretation, making it difficult to measure variables precisely. Lastly, any attempt to establish causality in the field of International Relations is necessarily limited by the complexity of international political phenomena. As such, it is never entirely possible to draw fully accurate generalisations about the behaviour of states. This study attempts to overcome these weaknesses through careful and transparent case selection, triangulation of data sources wherever possible, comparison of findings across different cases, and acknowledging the contingent nature of any predictions that emerge from the study.

1.7.3 Case Selection Criteria: Control, Variation, and Testability

This study employs a qualitative methodology and draws inferences about cyber strategy selection through an in-depth examination of three main cases: Brazil, the United States of America, and the Russian Federation. These three cases are examined during a period stretching from the early 2000s, when these states first began to systematically incorporate cyber power into their foreign policies, until 2022. This analysis period includes the early stages of the full-scale Russian invasion of Ukraine, which began in February 2022. The selection of these cases provides a global perspective, helping us to consider the phenomenon of cyber strategy selection across a diverse range of political and geographic contexts.

When using the case study methodology, the question of which cases to include in the research design is of great importance (George & Bennett, 2005, p. 83). Case study research seeks insight into a broad phenomenon by understanding specific instances of that phenomenon. Since the discipline of International Relations typically deals with small populations of units or events, finding cases that are truly representative or generalisable to a larger population can be challenging (Kacowicz 2004, p. 120). However, it is possible to partially overcome this limitation and make reasonable inferences by carefully selecting cases that provide the necessary level of control, variation, and testability. These three criteria have been used to guide the selection of cases for inclusion in this study.

The first criterion, control, refers to the need for some variables across the different cases to be held relatively constant in order to allow for consistent comparison. In the case of the three selected cases in the study, the most important is the fact that these are all major regional or global powers with significant potential cyber capabilities. While the United States and Russia are widely recognised as having significant cyber capabilities, Brazil is also a technologically sophisticated state that possesses numerous state agencies with competence in the cyber domain, as documented in Chapter Four. Achieving a perfectly controlled comparison in International Relations is rare, and the research design utilised in this study is not immune to this general problem. There are significant power differentials between the three selected cases, with the United States being notably larger than the other two cases in terms of its conventional military strength, the size of its technology sector, and the overall size of its economy. Nevertheless, the most important commonality between the three states is the fact that they all possess sufficient wealth and technological capability to make aggressive use of every dimension of cyber power, should they wish to do so.

The second criterion, variation, requires the selected cases to exhibit diversity, to ensure that there are distinct features in each case for the researcher to test and explain. Variation is typically easier to achieve than control criterion – especially in the field of International Relations, due to the inherent diversity and variation between different states. In this study, the cases were carefully chosen to ensure variation along the dependent variable of interest: their selection of cyber strategy. As Chapter Four on Brazil documents, Brazil is generally restrained in its use of all forms of cyber power. As such, Brazil serves an important negative case study in this research design, which helps observe and explain the non-use of cyber power. The Brazilian case also helps establish a baseline set of expectations that can be used to better understand the other two cases. By contrast, Russia and the United States have both been highly aggressive in their use of cyber operations. However, even between these cases, there is variation, with Russia employing unusually intensive online propaganda and disinformation.

In addition to these variations between cases, there are important longitudinal variations within each case. Brazil and the United States both underwent several changes in presidential administrations and governing parties during the historical period under consideration. Russia and the United States experienced significant changes in their geopolitical environment, shifting between periods of crisis, periods of war, and periods of relative peace. These within-case variations serve to further increase the number of observations in this study and help expand the explanatory leverage of this research.

There is another important sense in which this selection of cases provides for variation. While the United States and Russia are both longstanding established powers in international politics, Brazil is part of the Global South, and is typically considered to be an emerging power rather than an established one. By testing the theory in this study against the Brazilian case, and determining whether it is capable of explaining Brazil's approach to foreign policy in the cyber domain, we can have greater confidence in the validity of the overall results.

The third criterion, testability, refers to the need for sufficient data in the public domain to facilitate a comprehensive analysis of each case. Each of these three states has been extensively covered by investigative journalists, academic scholars, computer security researchers, and think tank researchers, providing a large volume of evidence in the public domain. This data can be used to estimate each state's capabilities and build up a profile of their operations in the cyber domain, allowing for in-depth analysis and meaningful comparison between the cases. Unfortunately, the

cases are not symmetrical in terms of testability: there is significantly more public data on the United States than the other two countries. For example, as the subsequent section on data collection notes, the news media in the United States regularly publishes investigative articles that give insight into the cyber capabilities of its intelligence agencies; by contrast, such reporting is far less common (though by no means nonexistent) in Russia. Nevertheless, Section 1.7.3 argues that there has been sufficient coverage of all three cases that it is possible to cross-reference and validate data points across different sources, thereby satisfying the testability criterion and strengthening confidence in the findings.

Overall, the selection of Brazil, the United States, and Russia allows for a comprehensive exploration of cyber strategies based on these three chosen criteria. The control criterion is met through their shared status as significant regional powers that possess significant actual or latent potential to carry out aggressive operations in the cyber domain. The variation criterion is satisfied by their differing approaches to cyber power. Finally, the testability criterion is met through the availability of public domain data on each state, thereby ensuring the robustness of the study's findings. The specific data sources used in this study are discussed in greater detail in the following section.

1.7.4 Data Collection Method: Triangulation of Qualitative Data

One of the major practical challenges in studying cyber power is the extreme level of secrecy that tends to surround this phenomenon. The unique conflict dynamics associated with zero-days create powerful incentives for secrecy; similarly, governments often prefer to avoid disclosing their involvement in online propaganda and misinformation campaigns in order to increase the effectiveness of these campaigns. The result is that, in the words of Clarke and Knake (2010, p. 2), cyber conflict is "shrouded in such government secrecy that it makes the Cold War look like a time of openness and transparency". To overcome this obstacle, this study employs a variety of primary and secondary sources in combination to shore up each other's weaknesses and tease out patterns of state behaviour in the cyber domain.

Much of the data that informs this study comes from investigative journalists who specialise in cyber security. Notable sources include David Sanger and Nicole Perlroth of the *New York Times*, Ellen Nakashima of the *Washington Post*, Andy Greenberg of *Wired,* Dan Goodin of *Ars Technica*, and freelance journalists Kim Zetter and Bruce Schneier. In particular, Andy Greenburg's (2019) investigations of the Sandworm APT, Max Seddon's (2014) reporting on the Internet Research Agency, Kim Zetter's (2014a) reporting on Stuxnet and SolarWinds, David Sanger and Ellen

Nakashima's reporting on the US intelligence community, Glenn Greenwald's (2014) reporting on National Security Agency (NSA) surveillance, Bruce Schneier's (2016b) reporting on encryption policy, and Fred Kaplan's (2017) history of the NSA are all invaluable resources. Investigative journalism is often informed by leaks from within government agencies, such as the information leaked by Edward Snowden. These leaks provide a rare and valuable window into government actions that would otherwise be inaccessible to scholars. However, investigative journalism also has several disadvantages. Leaked information provides a partial view of the truth; some stories are never leaked, while others are leaked on purpose to create a favourable impression of the government. Furthermore, investigative journalism tends to produce more stories about democracies than authoritarian states since the latter typically do not permit the press to operate freely (Buchanan, 2017a, p. 12). This can result in a form of selection bias, creating a misleading impression that cyber operations are used more frequently by democracies. As a result, investigative journalism must be supplemented with other sources.

A second source of data employed in this study is threat intelligence reporting from commercial cyber security firms. These companies, including FireEye, Kaspersky Lab, CrowdStrike, ESET, Symantec, and others, periodically release reports on specific actors, incidents, and threats in the cyber domain. Private security researchers possess a high level of expertise and play a major role in investigating sophisticated attacks such as Stuxnet, the Conficker worm, and the DNC hack (Alperovitch, 2016; Bowden, 2011; Zetter, 2014a). These sources come with their own set of pitfalls, however. Security companies and researchers have an economic incentive to inflate threats and exaggerate their levels of competence, and the language and concepts employed tend to be highly technical and inaccessible to non-specialists. Nevertheless, they remain an invaluable source of information on state behaviour. As Buchanan (2017a, p. 10) observes, "[o]ne cannot credibly claim to understand states' current approaches to cyber operations without examining this detailed evidence of actual behaviour".

In addition to commercial reports from cyber security firms, several research institutes and think tanks have published useful reports in the fields of online security and disinformation. The Atlantic Council, for example, has published a comprehensive study of the #MacronLeaks cyber operations, which is used in the case study on Russian cyber strategy (Vilmer, 2019). The RAND Corporation has published several in-depth reports on topics such as zero-day life cycles (Ablon & Bogart, 2017), incentives for conflict and deterrence in the cyber domain (Libicki, 2009), and the Russian state's approach to information warfare (Paul & Matthews, 2016), all of which are cited in this study.

However, while think tank research is a valuable source of primary evidence, there are disadvantages to using these sources. Both the RAND Corporation and the Atlantic Council, for example, are formally aligned with the interests of the United States, and their research tends to reflect US perspectives and priorities.

Government investigations are another vital primary data source used in this study. Government agencies have the power to compel witnesses and bring significant resources to bear on investigations, including the use of classified intelligence sources. As a result, government reports can be extremely useful research sources. This study makes use of several such reports, including the Mueller Report (2019), an extraordinarily detailed document that serves as the primary historical record of Russian interference in the 2016 US presidential election, and the US Senate (2019) report on Russian social media activity in the United States. It also cites a report by New Knowledge, a consultancy firm, that was commissioned by the US Senate (DiResta *et al.*, 2019). For information about the Russian intervention in the UK, this study makes use of the UK Parliament's (2020) report on Russia's activities in the cyber domain and its impact on UK national security. Furthermore, it considers the UK National Cyber Security Centre report on the Russian Main Intelligence Directorate (GRU), which offers a rare official source on the activities of Russian APTs (NCSC, 2018).

These reports are invaluable sources that help provide detail and clarity on issues that were previously subject to speculation. However, there are several problems with these sources. Many of these reports are released with redactions and rely on classified information that is impossible for researchers to independently verify. Furthermore, authoritarian states usually do not release investigative reports, while democracies typically only release reports on the activities of other actors, not their own intelligence agencies. This data source, therefore, suffers from the opposite bias to that found in investigative journalism: it creates the misleading impression that democracies do not engage in aggressive cyber operations.

To attempt to overcome the problem of selection bias in the data collection phase, this study uses several datasets and aggregators that aim to provide a comprehensive overview of state-sponsored cyber operations. The most useful of these are the Cyber Operations Tracker published by the Council on Foreign Relations (CFR, 2022) and the Significant Cyber Incidents List published by the Centre for Strategic and International Studies (CSIS, 2023). These aggregators attempt to provide an exhaustive list of every cyber operation carried out by every state in the world in any given year. However, they typically rely on investigative journalism and incident reports from cyber security

firms to provide their underlying data, which means that to some extent they reproduce the problems with these other types of sources. Furthermore, while these datasets aim to be comprehensive, they include only incidents that are in the public domain, which means that by definition, they exclude any cyber operations whose existence has been successfully kept secret. The CFR admits that its Cyber Operations Tracker "is still a work in progress", and "is incomplete" (Segal, 2017). Nevertheless, these datasets are very helpful for gaining a comprehensive understanding of cyber operations during particular historical periods and perpetrated by particular states.

This study also uses several other datasets that provide cross-national data on specialised topics. For information on defence spending, it uses data provided by the Stockholm International Peace Research Institute (SIPRI, 2022) (SIPRI). For data on social media usage, it relies on annual statistics published by We Are Social (2022), a digital marketing agency that compiles reports on social media usage. For comparative data on social trust, it makes use of the Trust Index published by Edelman (Edelman, 2022), a US-based public relations firm. Lastly, for a comprehensive cross-national understanding of persuasive cyber power usage, this research draws upon the Oxford Internet Institute's Computational Propaganda Project, which attempts to create a complete record of the use of social media disinformation campaigns across different states.

Some countries, including the United States (2018) and Brazil (2008); (Brazil, 2018), publish formal cyber strategies. These documents were evaluated while writing this study and are cited in relevant parts of this text; however, they are not heavily used as data sources. These documents tend to provide a highly sanitised view of government views on the cyber domain. In contrast, this study is primarily focused on analysing and explaining patterns of state behaviour in practice.

Finally, this study incorporates ideas from secondary sources, including other scholars who have evaluated the above data sources and drawn their own conclusions from the results. This body of scholarly literature is reviewed in Chapter Two of this study.

The data sources utilised in this research all have different strengths and weaknesses. However, many of these sources are complementary and help to compensate for each other's shortcomings. Investigative reports published by democratic governments aid in understanding the activities of authoritarian states, while investigative journalists help reveal the actions of democracies. Leaks, such as those from Edward Snowden, provide insight into the inner workings of governments. Threat intelligence reports offer technical details on the cyber operations of states, while secondary

resources from scholars help to understand the large-scale strategic objectives that motivate these operations. Aggregate datasets, which focus on providing a comprehensive overview of state-sponsored cyber operations throughout the world, help to counteract the problem of data selection bias. By combining these data sources and triangulating between them, this study attempts to address the weaknesses of each individual data source. Although the problem of secrecy is impossible to fully overcome, this approach has sought to develop a reasonably complete and accurate picture of the cyber strategies of the three countries used as case studies.

1.7.5 Data Analysis Method: Congruence Testing and Cross-Case Comparison

Data from the above sources was analysed in this study using a combination of the congruence method and cross-case comparison. The congruence method is an approach in which a theory is first developed using the logic of deduction, and cases are then selected and tested to determine whether they align with the predictions of the theory. George and Bennett (2005, p. 181) describe the essential characteristic of the congruence method as follows:

> The essential characteristic of the congruence method is that the investigator begins with a theory and then attempts to assess its ability to explain or predict the outcome in a particular case. The theory posits a relation between variance in the independent variable and variance in the dependent variable; it can be deductive or take the form of an empirical generalization. The analyst first ascertains the value of the independent variable in the case at hand and then asks what prediction or expectation about the outcome of the dependent variable should follow from the theory. (George & Bennett, 2005, p. 181)

In this study, a set of three relevant cases characterised by variation along the dependent variable – Brazil, the United States, and Russia – is examined. An in-depth analysis of these cases is conducted to confirm and classify the nature of their respective cyber strategies. Based on the theoretical framework, predictions are made about the values of the independent variables – the external security requirements and institutional preferences – that would likely be found in each case. Finally, each case is evaluated to determine whether the empirical data is congruent with the expectations of the theory.

In addition to the congruence method, the cases are further evaluated using a process of cross-case comparison, employing a most-similar research design. This method of comparison, also known as

Mill's method of difference, is a useful tool for explaining cases with different outcomes. George and Bennett (2005, p. 157) describe the method as follows:

> In the method of difference—in which two cases having different outcomes are compared—the investigator employs the logic of elimination to exclude as a candidate cause (independent variable) for the variance in the outcome (dependent variable) (George & Bennett, 2005, p. 157).

The most-similar research design is used in this study because the selected cases share significant similarities, while also having important differences in their cyber strategies (the dependent variable) and their external security requirements and institutional preferences (the independent variables). All three of the selected countries are prominent regional powers with considerable cyber capabilities. However, the cyber strategies adopted by these countries vary greatly, both in terms of their focus on technical or persuasive cyber power and their level of aggression. The use of this design helps to control for cyber capability as a potentially confounding variable, allowing us to eliminate it from consideration. Furthermore, as these cases greatly differ in their security requirements and approach to international relations, this method enables us to further test the plausibility of the hypothesis that these two factors contribute to explaining the cyber strategies of these respective states.

In combination, the congruence method and cross-case comparison offer a thorough and robust analysis of the available data, providing strong evidential support for the hypotheses presented in this study.

1.8 Chapter Outline

In conclusion, this chapter lays the foundation for this study. It states the research question and outlines the expected thesis of this study. It clarifies the empirical focus of this study by defining contested terms such as "cyber domain" and "cyber power." Furthermore, it provides a list of technical terms dealing with computer security and social media, which are referenced throughout the remainder of this text. It highlights key theoretical assumptions that underpin this study, drawing primarily from realist theoretical approaches in the field of International Relations. Finally, it outlines the research methods used to complete the study, including the selection of case studies, data collection, and the analysis methods that are used to answer the research question. The

remaining chapters build upon these foundations to develop a theory of cyber power in international politics.

The second chapter examines the previous literature on cyber power in international politics and situates this study within this broader body of scholarship. It argues that it is possible to distinguish three main schools of thought on this topic: transnationalism, constructivism, and realism. While this study is located within the realist school of thought on cyber politics, it attempts to extend it by moving from descriptive to explanatory theorising.

The third chapter constitutes the theoretical core of this study. It argues that cyber power can be conceptually divided into two subtypes: technical cyber power, which undermines trust in technical systems, and persuasive cyber power, which undermines trust in institutions. By examining the trade-offs states face when using both forms of cyber power, it becomes possible to develop a typology of strategies available for states to select. This chapter argues that states are likely to choose their strategy based on their external security requirements and their institutional preferences, which influence their willingness to accept these trade-offs.

The fourth, fifth, and sixth chapters attempt to test this theory by examining the cases of Brazil, the United States, and Russia, respectively. These chapters argue that Brazil has adopted a "restrained strategy", while the United States has embraced a "technical-aggressive" strategy, and Russia has chosen a "combined-aggressive" strategy. With each case, these chapters aim to uncover the relationship between these cyber strategies and the underlying security requirements and institutional preferences that motivate these states.

Finally, the seventh chapter ties together the study, summarising and comparing the findings of the case studies while arguing for the validity of the realist theory of cyber power. This chapter makes several predictions regarding the countries examined in the study and discusses possible future scenarios in which shifts in independent variables lead to corresponding changes in cyber strategies. Finally, it points out that the realist theory of cyber power has several unpleasant implications. If certain global trends continue, the theory predicts that we are likely heading toward a world in which both our technical systems, and even our perception of the truth, are increasingly subject to attacks by sovereign states.

Chapter 2
Literature Review:
The Quest for a Theory of Cyber Politics

2.1 Introduction

This study aims to develop a theory of cyber power in international relations. To explain how this theory differs from previous ones and how it builds upon existing scholarship, it is necessary to understand the broader body of academic work that focuses on cyber politics as a phenomenon in international relations. To this end, this chapter reviews this body of literature and traces earlier attempts to construct such a theory. It argues that most of the literature in the subfield can be divided into three broad schools of thought: transnationalism, constructivism, and realism.

Political scientists who study cyber politics hold diverse theoretical viewpoints and normative commitments, but most seem to agree on the importance of the theory-building project itself. Valeriano and Maness (2015, p. 17) argue that "thoughtful theoretical analysis... is sorely needed"; Kello (2017, pp. 7-8) suggests that theories are needed to "yield strategic insight" and "mitigate new threats". Choucri (2012, p. 16) argues that IR theory must account for "the intersection of the kinetic and the constructed cyber". Yet, most scholars also argue that our existing theories are incomplete and unsatisfactory. Kello (2017, p. 9) argues that existing scholarship "barely, and sometimes not at all, integrates the virtual weapon into the theoretical matter of international relations". Valeriano and Maness (2015, p. 42) complain that "the main flaw of the entire cyber security enterprise is a complete lack of theoretical engagement". Choucri and Goldsmith (2012, p. 75) lament the "enormous disconnect between the cyber realities of today and the theories of the twentieth century". Eriksson and Giacomello (2006, p. 222) suggest that "past research on this topic has been idiosyncratic and policy-oriented, with little or no effort made to apply or develop theory".

This chapter challenges this view. It argues that there has been a relatively sustained attempt, starting in the early 1990s and continuing to the present, to develop theories of cyber power. The results of these efforts are three nascent schools of transnationalism, constructivism, and realism.[8]

[8] Previous scholars have developed other classification schemes and meta-theories to describe how cyber politics is understood within IR. Eriksson and Giacomello (2006) argue that the "information revolution" can be understood using the three dominant theoretical perspectives of IR: realism, liberalism, and constructivism. Manjikian (2010) argues that cyber conflict can be understood through three theoretical lenses: realist, liberal,

Each of these schools makes somewhat different assumptions about the relationship between cyber power and international politics. A summary of the three schools can be seen in Figure 2.

Each of these schools of thought is internally diverse and there is significant disagreement within them. However, each school contains an important insight at its core. The core insight of the transnationalists is that cyber space transforms the international system by increasing the number of actors and the complexity of interactions. Among sovereign states, cyber space diffuses power away from stronger states and empowers weaker ones; more broadly, it empowers non-state actors over states. Cyber space is also seen as creating new forms of interaction, separate from the traditional tools of statecraft such as war or diplomacy.[9]

Constructivism is a theory of International Relations that emphasises the importance of identities, discourses, and norms. The core insight of the constructivist school of cyber politics is the danger of securitising the discourse on cyber space. From this perspective, the "threats" articulated by the other two schools are overblown and threaten to militarise what was once a liberating space for civilian communication. By rejecting these inflated threats, it argues, and by strengthening international norms of cyber restraint, we can avoid this outcome.

Finally, there are the realists. The core idea of this school is the centrality of the state, even in the cyber domain. By making this assumption, realists hope to apply many of the conceptual tools of traditional IR theory to the study of cyber politics. Contrary to the stereotype, the realist view is not necessarily pessimistic. Some scholars in this school assume there is potential for stable balancing behaviour in the cyber domain, and some even suggest that cyber power might give states a useful way to engage in rivalry without physical violence (Rid, 2013). However, all realists agree that states remain the central actors in the domain.

---

and utopian. Langø (2013) identifies three major schools of thought: revolutionist, traditionalist, and environmentalist.

[9] It is important to note here that "transnationalism", as I have identified it here, is not simply the cyber counterpart of "liberalism" in International Relations. Unlike conventional liberalism, the transnationalist school of cyber politics is not necessarily optimistic about the trends it identifies. Some of the authors in this group (for example, Rosecrance) are indeed optimistic, but others (eg. Kello) are pessimistic, and others still (eg. Nye) are ambivalent. In addition, this perspective is missing one very important component of the traditional liberal approach to IR: a focus on institutions. Due to both technical and political challenges, international cyber issues are weakly institutionalised, and it is not yet clear whether it is possible to create strong international institutions or regimes to govern them. This study includes a heavy focus on institutions; however, it treats institutional preferences as a dependent variable used to explain cyber strategy selection, rather than treating international institutions as an independent variable that is likely to mitigate cyber conflict. See Chapter Three for a more detailed discussion of this topic.

The remainder of this chapter explores the underlying assumptions of these three schools of thought, and the different ways they try to explain and predict politics in cyber space. It also identifies some of the major areas of disagreement within each school, and the ways in which these schools have developed and evolved. Existing theories on cyber power face several shortcomings, primarily their inadequate consideration of both instrumental and persuasive aspects of cyber power. This limitation is due, in part, to the general lack of focus on the potential for state-level variations in the utilisation of cyber power. Most existing theories emphasise the overall impact of cyber power on the international system, rather than exploring the distinct incentives that different states may have depending on their strategic context. Consequently, these theories do not adequately explain the variations between the cyber strategies of states.

	Transnationalism	**Constructivism**	**Realism**
Principal unit of analysis	States and transnational actors	Norms and ideas about cyber security	States
Explanatory processes	Power diffusion	Threat inflation	Conflict under anarchy
Effects of cyber space	Increased complexity of interactions	Generally benign	New foreign policy tools for states
Beneficiaries	Weaker states and non-state actors	Security elites within states	Stronger states
Patterns of conflict	Complex mix of states and non-state actors	States vs. their own citizens	States vs. states
Major risks	Disruption of international order	Overreaction by states and security elites	Miscalculation and escalation
How to prevent cyber conflict	Interdependence	Norms of restraint	Innovative deterrence mechanisms

Figure 2: Summary of the major schools of thought identified in this chapter.

2.2 Transnationalism: New Actors and Interactions

At its core, "transnationalism" is the view that IR theory should incorporate non-state actors as units of analysis. This apparently simple idea is, in fact, a significant departure from the dominant tradition in International Relations, which is to treat states as aggregate units (Lake, 2008, pp. 41-46). Transnationalism can thus be contrasted with the more traditional research programmes of neo-realism and liberal institutionalism, which dominated the field of IR for much of the post-World War II era (Barnett & Sikkink, 2008, p. 70). Those theories tend to view the international system as an

arena for the strategic interactions of sovereign states and focus on discovering the conditions that lead to peace or war among them.[10] However, starting in the early 1970s, an increasing number of scholars, including Rosenau (1969), Kaiser (1971), and Nye and Keohane (1971b), began to challenge the state-centric model of international politics. They argued that developments in international communication, transportation, and trade have empowered a new class of "transnational" actors - multinational corporations, religions, rebel groups, trade unions, epistemic communities, advocacy networks, and so forth (Lake, 2008, p. 48; Nye & Keohane, 1971b, p. 331). Lake (2008, p. 48) argues that transnationalism does not simply add a new set of actors to the analytical mix. Instead, it constitutes a "substantive critique of state-centric theory", which makes the claim that the international system has been fundamentally reshaped by economic and technological processes that reduce the agency of states (Lake, 2008, p. 48).

In their classic statement on transnationalism, Nye and Keohane (1971b) make three major arguments in support of this position. First, they assert that state-centric models of the international system are self-evidently incomplete and limited. Second, they point out that transnational actors, though mostly based within sovereign states, are capable of forming independent relationships with states and each other, thereby creating a complex web of strategic interaction at the international level. Third, they argue that transnational actors can influence international outcomes, including war and peace, by altering the decision-making incentives facing states. While the existence of transnational actors is not a novel phenomenon (for instance, the Catholic Church has been an influential actor for centuries), this capacity to push the international system toward greater levels of war or peace is a more recent development (Nye & Keohane, 1971a, pp. 724-725). Nye and Keohane tend to regard this as a good thing: they argue that transnational interaction encourages cosmopolitan thinking, domestic pluralism, interdependence between states and, ultimately, a reduced likelihood of war (Nye & Keohane, 1971b, p. 337).

The early transnationalists explicitly argued that the shift in power from states to non-state actors is driven, in part, by advancements in global communications technology. For instance, Nye and Keohane define four means by which transnational groups interact with the world. The first of these is "communication, the movement of information, including the transmission of beliefs, ideas, and doctrines", which requires advanced technology (Nye & Keohane, 1971b, p. 332). As the internet grew in the 1990s, it seemed to validate the assumptions of the early transnationalists. Much of the early political commentary on the significance of the internet – which often took place outside of

[10] For example of state-centric theorising in IR, see Waltz (1979), Robert O. Keohane (1984), and Wendt (1999).

academic circles – was radically libertarian and transnational in its orientation. The most famous example of this "cyber utopian" position is *A Declaration of the Independence of Cyberspace*, a political manifesto published by John Perry Barlow – an American political activist, poet, cattle rancher, and co-founder of the Electronic Frontier Foundation (Jarnow, 2018). Incensed by the 1996 Telecommunications Reform Act in the United States, Barlow argued that the internet would soon render states obsolete. In his manifesto, Barlow writes the following:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. (Barlow, 1996)

Barlow took it for granted that the arrival of the internet would weaken the power of states.[11] Today, his rhetoric seems unrealistic and naive. We have since discovered that authoritarian states, such as China and Iran, have considerable capacity to monitor and restrict internet usage by their citizens (August, 2007). And, even in Western democracies governments have figured out how to regulate and surveil the internet. Furthermore, some observers have come to question the normative assumptions of "internet freedom", worrying that memetic selection and transmission of ideas on social media networks might potentially be corrosive to democracy (Tufekci, 2018). As a result of these developments, the transnationalist literature on the internet has retreated from its early optimism and became more ambivalent about the trends it identifies.

This transformation mirrors the broader changes in transnationalism as a school of thought in International Relations. The original transnationalists tended to be positive about the changes they identified. Barnett and Sikkink (2008, p. 72) argue that early transnationalist scholarship has a "liberal bias", since it tends to assume that diffusion of power in the international system away from states is inherently a force for good. However, a second wave of literature on the dark side of transnationalism began to explore "dark networks" operated by criminal organisations and terrorists

[11] A more nuanced discussion of the emancipatory potential of the internet, from approximately the same era, can be found in Lessig (1999).

(Barnett & Sikkink, 2008, p. 72). This concern – that the shift in power towards non-state actors might be threatening and destabilising – is also evident in the transnationalist literature on "cyber war".

2.2.1 Arquilla & Ronfeldt: Transnationalism & Networks

The first researchers to systematically consider the impact of the internet on international conflict were John Arquilla and David Ronfeldt. In 1993, writing under the auspices of the RAND Corporation, they introduced a new phrase into the lexicon of political science: "cyber war" (Arquilla & Ronfeldt, 1993). They developed and refined their ideas in a series of subsequent works (1996, 1997b, 2001), and these writings constitute the first real attempt at developing a comprehensive transnationalist understanding of cyber politics. Many of their assumptions continue to permeate the subsequent scholarship on the topic. However, their starting viewpoint differs significantly from liberal transnationalists such as Nye and Keohane. Arquilla and Ronfeldt's goal is not to formulate a general theory of international politics in cyber space. They do not attempt to apply their framework to situations of cooperative relations between countries, and they lack the optimistic assumptions of the liberal transnationalists. Instead, their focus is almost entirely on warfare and the national security of the United States.

The 1993 article by Arquilla and Ronfeldt that introduces the concept of "cyber war" contains relatively little discussion of computers and does not even mention the internet.[12] Instead, they discuss the importance of information in the context of conventional warfare. They argue that the mastery of information, in the form of superior command, control, and communications networks, is a force-multiplier that gives smaller armies the ability to defeat larger opponents.[13] At the time of writing, they assume that information technology will influence international relations mostly by giving state-based military forces more freedom to manoeuvre on the battlefield. Nevertheless, they argue that information technology might also facilitate conflict "between governments and non-

[12] Arquilla and Ronfeldt tend to be sceptical of the transformative power of technology itself. They admit that "new technologies make possible a rather 'pure' variety of netwar" in which all conflict takes place within cyber space (Arquilla & Ronfeldt, 1997b, p. 285). However, they expect that such conflicts will be relatively rare, and will not deliver decisive victories to any side even when they do occur.

[13] Arquilla and Ronfeldt discuss the Carthaginian army of Hannibal Barca, and the Mongol armies of the Great Khans, as historical examples of military forces that managed this form of information dominance. They even argue that "[t]he Mongol way of warfare, which reached its zenith in the twelfth and thirteenth centuries, may be the closest that anyone has come to waging pure cyberwar" (Arquilla & Ronfeldt, 1993, p. 148), which illustrates how this terminology has evolved over time.

state actors", and suggest that non-state actors may be "organised [through the use of technology] into vast transnational networks and coalitions" (Arquilla & Ronfeldt, 1993, p. 145).

In later works by Arquilla and Ronfeldt (1996, 2001), non-state actors take centre stage. Information technology, they argue, makes it easier for non-state actors to organise themselves into networked structures. "Networks" are regarded as one of four major types of organisation, and are contrasted with hierarchies, markets, and tribes (Arquilla & Ronfeldt, 1996, p. 25). Networks are defined as collections of dispersed nodes, linked together through channels. Compared to hierarchical actors (e.g. states), networked actors display high levels of flexibility, resilience, and tactical innovation (Arquilla & Ronfeldt, 1997a). This makes them capable actors in international conflict. Indeed, Arquilla and Ronfeldt (2001) argue that networked non-state actors tend to inflict defeats upon state-based opponents relatively often, even when they are inferior in terms of conventional military strength.[14]

In practice, various types of non-state actors make use of this networked structure. The list of networked non-state actors includes terrorist groups and criminal organisations, but it also encompasses "civil-society activists fighting for democracy and human rights" (Arquilla & Ronfeldt, 2001, p. i). They stress the idea that "netwar [has] two major faces, like the Roman god Janus – one dominated by terrorists and criminals that is quite violent and negative, and another evinced by social activists that can be militant but is often peaceable and even promising for societies" (Arquilla & Ronfeldt, 2001, p. 1). While they are ambivalent about whether the trend is beneficial, they are quite clear that it is changing the structure of international politics. Since hierarchies struggle to fight against networks, the overall effect is that "power is migrating to non-state actors" (Arquilla & Ronfeldt, 2001, p. 1).[15]

Apart from the concept of "cyber war" (which evolved into a rather different concept in the hands of subsequent scholars), Arquilla and Ronfeldt's most important contribution is to provide a new image of world politics. This is a world in which non-state actors, organised into networks and empowered

[14] They cite Hamas, the Cali cartel, the Zapatista movement in Mexico, and the International Campaign to Ban Landmines as examples of networked non-state actors that have challenged states, and met with at least some success (Arquilla & Ronfeldt, 2001, pp. 15-16).

[15] Interestingly, Arquilla and Ronfeldt also discuss the importance of "soft power" in modern conflict. They predict that propaganda, intelligence, and psychological manipulation will emerge as decisive factors in determining who wins in the kinetic sphere. "Conflicts", they argue "will increasingly depend on, and revolve around information and communications... [Conflict is] about who knows what, when, where, and why, and about how secure a society, military, or other actor is regarding its knowledge of itself and its adversaries" (Arquilla & Ronfeldt, 1996, p. 5).

by technology, are increasingly capable of challenging states. To be sure, the key intervening variable in the Arquilla and Ronfeldt's framework is the networked organisational structure, rather than the internet or any other form of technology. Furthermore, their approach to security studies is fairly conservative, in the sense that their overarching concern is the national security of the United States as a political unit. Nevertheless, their arguments fall within the broader transnational school, since they assume that the effect of information technology is ultimately to transfer power away from states. Moreover, their ambivalence about this trend, which is seen as both threatening but also (at least potentially) progressive, is typical of how later transnationalists would come to view the cyber domain.

2.2.2 Rosecrance, Keohane, and Nye: The Liberal Transnationalists

While Arquilla and Ronfeldt were developing their concepts of "cyberwar" and "netwar" in the early 1990s, the broader discipline of IR was going through a dramatic period of self-reflection and debate (Holsti, 1998, p. 2). For many scholars, the unexpected (and largely peaceful) end of the Cold War undermined the credibility of the discipline's two dominant paradigms, neo-realism and neo-liberalism (Kegley, 1993; Lebow, 1994; Sindjoun, 2001). Seizing on the moment, scholars offered up a succession of "big ideas" that purported to explain some aspect of the new post-Cold War world politics (Fukuyama, 1989; Huntington, 1993; Mearsheimer, 1990; Nye, 1990). At the same time, new theoretical perspectives such as constructivism and post-modernism critiqued the established theories for their alleged rationalism, materialism, and claims to scientific objectivity (Devetak, 1999; Wendt, 1992).

This decade was also the period in which International Relations scholars first grappled with the emergence of the internet. At the time, many liberal scholars argued that the internet reinforced trends towards economic globalisation, which in turn validated liberal concepts such as complex interdependence and transnationalism (Orenstein & Schmitz, 2006). Among the first liberal scholars to make this connection was Rosecrance (1996, 1999, 2002), with a series of articles that predict the rise of the "virtual state". This argument extends Rosecrance's earlier (1987) theory of "trading states", which argues that the modern economy has reduced the benefits that states obtain from waging war while increasing the benefits they receive from peaceful trade.[16] For Rosecrance (1996),

[16] The countries that most epitomise this dynamic are Japan and Germany, both of which sought gains through violent territorial expansion in World War II. After being brought to the brink of ruin at the end of the war, they both shifted to a "trading state" strategy in the post-war era and achieved high levels of economic successes.

the internet reinforces this dynamic. The globalised economy, he argues, is characterised by high levels of capital, labour, and information mobility. Just as multinational corporations are able to split their operations across different countries, entire states can now specialise in one link of the production chain, such as intellectual property development or manufacturing (Rosecrance, 1996, p. 46).[17] This reduces the incentive to acquire fixed resources, such as territory or natural resources, which in turn reduces the risk of war and violent conflict (Rosecrance, 1996, pp. 56-57).

Rosecrance was followed by Keohane and Nye, who had previously argued that economic incentives would drive self-interested states towards greater levels of cooperation (Keohane & Nye, 1973). In a 1998 article, they extend this argument, suggesting that cheap and instantaneous cross-state communication was strengthening non-state actors and creating new classes of transnational actors. Previously, the most powerful non-state actors had been hierarchical organisations, such as business corporations or the Catholic Church (Keohane & Nye, 1998, p. 83). However, they argue that the internet strengthens non-traditional non-state actors, such as non-governmental organisations (NGOs) and transnational advocacy networks, which then become "effective in penetrating states" and shaping state preferences (Keohane & Nye, 1998, p. 83). Examples of such non-traditional actors are Greenpeace, the International Campaign to Ban Landmines, and the Intergovernmental Panel on Climate Change (Keohane & Nye, 1998, p. 92).

Nevertheless, Keohane and Nye predict that states will eventually figure out ways to use technology for their own advantage. Information technology, they argue, will become an important power resource and will serve as a foundation of military strength, in the same way that agricultural technology once provided the manpower for infantry armies (Keohane & Nye, 1998, p. 87). They predict that *status quo* powers, such as the United States, are likely to retain their technological advantages, and the spread of information technology will not increase the relative power of smaller states (Keohane & Nye, 1998, p. 88). They predict that the internet will increase the ability of states to use propaganda in support of their foreign policy goals, and point out that in a world of "information abundance", credible aggregators of information will wield enormous influence (Keohane & Nye, 1998, p. 89).[18] However, they assume that this will benefit liberal democracies;

[17] For example, states such as Switzerland, Japan, and Singapore are able to become wealthy and successful by cultivating their human capital and producing knowledge, while outsourcing the manufacturing of goods to other states, such as the People's Republic of China (Rosecrance, 1996, pp. 52-53). It should be noted that this is a direct challenge to the theories of Waltz (1979), who argues that states are unable to specialise due to the constraints of international anarchy.

[18] In their argument, Keohane and Nye accurately predict the power of information aggregators such as Facebook: "A plenitude of information leads to a poverty of attention... Editors, filters, interpreters, and cue-

they did not anticipate the possibility that illiberal states such as Russia might use persuasive cyber power to advance their own interests.

The relationship between the internet and "soft power" is discussed in more detail by Nye, in a series of articles on the future of power (2010, 2011a, 2011b). The effect of cyber power, Nye argues, is not to tilt the balance from one strong state towards another. Rather, it is to diffuse of power away from all the strong states, while benefitting smaller states and transnational actors (Nye, 2010, p. 1). "[T]he barriers to entry in the cyber domain," he argues, "are so low that non-state actors and small states can play significant roles at low levels of cost" (Nye, 2010, p. 4). According to Nye (2010, p. 9) several classes of transnational actors are able to wield significant levels of cyber power: multinational technology corporations; criminal organisations; individual hackers; and potentially, terrorist groups. These smaller actors enjoy certain asymmetric advantages, since they have fewer assets to defend, lower costs, and are less dependent on vulnerable electronic systems (Nye, 2010, p. 13). They also benefit from the internet's lack of physical distance and imperfect governance by a patchwork of different authorities (Nye, 2010, pp. 4, 15).

Nevertheless, Nye (2010, p. 13) stresses that states are also capable of wielding cyber power, and argues that "[g]overnments are top dogs on the internet"; something that is especially true for powerful states such as the United States, Russia, Britain, France, and China (Nye, 2010, p. 4). Overall, Nye's own writings on cyber power are less optimistic and accord more agency to powerful states than his co-authored writings with Keohane. In this regard, Nye acts as a bridge to the realist school, which is discussed in greater detail in Section 2.4 of this chapter.

2.2.3 Choucri: Lateral Pressure in Cyber Space

The theorists examined in previous sections focus on one particular aspect of international politics: conflicts between networked actors (Arquilla and Ronfeldt); global division of labour (Rosecrance); complex interdependence (Keohane and Nye); and soft power (Nye). By contrast, Choucri (2012) attempts to develop a grand theory of international cyber politics.[19] Her theory describes and

---

givers become more in demand, and this is a source of power." However, they argue that mainstream news sources are more likely to be seen as credible, since they produce information "through a process that is in accordance with professional norms and characterized by transparency and procedural fairness" (Robert O. Keohane & Nye, 1998, p. 92). They do not anticipate the fractalising effects of social media, in which audiences are split into ever-smaller echo chambers that are reinforced by algorithmic filter bubbles.

[19] See also Choucri (2015), Choucri, Madnick, and Ferwerda (2014), Vaishnav, Choucri, and Clark (2013), and Choucri and Goldsmith (2012).

explains a broad range of behaviour in cyber space, including the rise of non-state actors, the emergence of new security threats, power diffusion, conflict, cooperation, institutionalisation, and the empowerment of individuals (Choucri, 2012, pp. 223-226). As a result, her approach is arguably the most complete articulation of the transnational school of cyber politics.

Choucri's (2012) theoretical approach is complex: incorporates numerous explanatory variables (including three "master variables"), classifies states into six "profiles", and attempts to integrate four levels of international politics. This theory does not aim for parsimony and is geared towards detailed description rather than prediction. Nevertheless, her conclusions are broadly compatible with the transnational school. Her core argument is that the internet challenges the traditional, state-centric view of international relations. In conjunction with Goldsmith (2012, p. 70), she argues that "[i]nternational relations theory, analysis, policy, and strategy were derived from experiences in the nineteenth and twentieth centuries and, therefore, were built on the assumptions that states are the relevant entities in world politics... But some critical features of cyberspace do not correspond with this traditional view of the state system". In common with other transnationalist writers, her assumption is that cyber space is transforming the international system by creating new transnational actors, empowering existing non-state actors, and diffusing power away from the strongest states.

Choucri's theory of cyber politics is derived from her broader theory of international relations, which she refers to as the theory of lateral pressure. She defines "lateral pressure" as the innate tendency of all human societies and organisations to expand, grow, and come into conflict with each other (Choucri, 2012, p. 25). States that generate unusually high levels of lateral pressure are typically described as being "powerful" in traditional theories of International Relations; Choucri (2012, p. 40) views power and lateral pressure as highly correlated, although not perfectly synonymous. A state's lateral pressure is driven by its population growth, its stock of natural resources, and technology, which Choucri (2012, p. 31) defines as three "master variables". By combining these variables, she argues, we can identify six "profiles" of states, which roughly predict their grand strategy selection (Choucri, 2012, p. 32).

In some respects, this theory is similar to realism, since it assumes that there is a built-in tendency for all states to come into conflict with each other. However, there are several differences between the lateral pressure approach and traditional realist approaches. Choucri does not view conflict as either an irrational psychological impulse or as a rational response to anarchy at the systemic level.

Instead, she argues that aggregate international behaviour can be traced back to individual human beings, and their propensity to process information and consume energy. According to Choucri (2012, p. 41), all human organisations generate lateral pressure, including sub-national and transnational organisations. In addition, while she adopts the three levels of analysis introduced by Waltz (1959), she also inserts a fourth level: the global level, situated above the level of the state system (Choucri, 2012, p. 45). This level is seen as encompassing the earth's natural environment, its energy resources, and global common spaces (including cyber space).

Within this framework, how does the existence of the cyber domain affect international politics? Like many previous scholars, Choucri argues that cyber power has the effect of empowering transnational actors and challenging the power of states (Choucri, 2012, p. 126). Corporations have an innate tendency to grow and expand, just like states do, and cyber space is a venue in which they are able to compete for influence and generate lateral pressure (Choucri, 2012, p. 40). More worrying, from the perspective of states, are challenges such as cyber crime, cyber espionage, cyber terrorism, and the possibility of cyber attacks against critical infrastructure (Choucri, 2012, pp. 143-153). She argues that the internet is particularly threatening for authoritarian states, since it provides a mechanism for citizens to communicate with each other, oppose the government, and organise peaceful protests or violent rebellion (Choucri, 2012, pp. 138-142).

However, there are also aspects of cyber space that strengthen states. States can build their capacities by engaging in "e-governance", using the internet to encourage political participation, identify aggregate preferences, and improve the quality of their services (Choucri, 2012, pp. 36-37). The internet also stimulates long-term economic development, which in turn provides the wealth that states use to fund their foreign policy strategies (Choucri, 2012, pp. 71-77). Furthermore, while the internet does create threats and vulnerabilities, it also creates a new security role for states to fulfil: the provision of cyber security (Choucri, 2012, pp. 38-39). State militaries have rushed to build up their capabilities and take on this new role, resulting in a trend that many observers find somewhat disconcerting: the "militarisation of cyber space" (Choucri, 2012, p. 148).

Inevitably, these trends mean that conflicts in cyber space will not exclusively take the form of states fighting against non-state actors; there will also be cases of states fighting other states. Choucri (2012, p. 127) identifies three types of issues that are likely to provoke such conflicts: disputes over the architecture and governance of the internet itself; competition for political and economic advantages on the internet; and the use of cyber power to achieve national security goals. There

have been a number of efforts to mitigate these conflicts, by adapting existing institutions or creating new forms of governance and norms for cyber space (Choucri, 2012, pp. 158-172). However, these efforts at institution-building are still in their infancy.

Choucri identifies several possible scenarios that might result from these processes: an internet that fragments into separate networks controlled by individual states; an anarchic internet that resists outside control; an internet that is managed by civil society as a global commons; or an internet that is governed cooperatively by states (Choucri, 2012, pp. 234-235). What is clear, from her perspective, is the inability of state-centric theories to explain these changes.

2.2.4 Kello: Transnationalism and Transformation

Kello (2013, 2014, 2017) is the most forceful advocate of the view that cyber space is not merely transnational but transformative, requiring us to fundamentally rethink many of the foundational concepts in IR. Concepts such as "anarchy", "order", and "system", he argues, allow us to grapple with complexity and construct useful theories, but they are overlaid on a material world that can be changed by new technology (Kello, 2013, p. 12). For example, the development of nuclear weapons altered many of the structural incentives that govern international politics, and Kello (2017, p. 4) argues that cyber power is likely to be even more transformative.

At the time of Kello's book-length treatment of the subject (2017), the debate on cyber politics in IR had advanced considerably. The debate was no longer among different camps of transnationalists. Constructivists and realists had taken notice of the discussion and begun to critique the more expansive claims of the transnationalists regarding the dangers and transformative potential nature of cyber power.[20] In response, Kello sharply criticises these authors – especially the so-called "Clausewitzian" theorists[21] - for their alleged "scientism", defence of traditional models, reliance on past behaviour to predict future trends, and failure to imagine revolutionary change.

Kello argues, in opposition to these authors, that the internet has significant potential to disrupt the existing international order. This disruptive potential stems partially from a "large-N" problem: the cyber domain is increasing the number of relevant actors in international politics and the complexity of their interactions (Kello, 2013, p. 35). In one sense, this is a restatement of the argument that

[20] See for example Gartzke (2013), Rid (2013), and Valeriano and Maness (2015).
[21] This study instead refers to this group of scholars as "sceptical realists".

transnationalists have been making since the writings of Arquilla and Ronfeld. However, Kello points out that cyber space not only empowers non-state actors. Instead, he argues, it diffuses power simultaneously at all levels of the international system: from the United States to Russia and China; from *status quo* states to revisionist challengers; and from states in general to transnational actors (Kello, 2013, pp. 35-37).

Furthermore, he argues that there are several features of cyber power that are intrinsically destabilising. These include offensive dominance and the attribution problem, both of which might tempt governments to seize a temporary advantage by attacking first (Kello, 2013, pp. 32-33).[22] Information technology is also volatile and difficult to incorporate into long-term planning, and computer networks offering poor strategic depth in defence. Finally, state policies on escalation are secretive and ambiguous, creating confusion about the circumstances under which a state might escalate from the cyber to the kinetic domain (Kello, 2013, pp. 33-34). All of these factors impede rational decision-making, increasing the risk that states in a hypothetical cyber crisis might cross an unspecified red line and trigger a war.

Kello (2017, p. 85) suggests three benchmarks that we can use to measure the extent to which any new technological advance may disrupt the international system. In order of severity, these are 1) systematic disruption, 2) systematic revision, and 3) systems change. Systematic *disruption* is the most moderate of the three outcomes and occurs when technology alters the balance of power within the existing order.[23] This is potentially worrying for individual states, but it can be mitigated and does not threaten the underlying moral foundations of the international order. Rational states might reduce the dangers by building new institutions, strengthening norms of non-aggression, or creating new forms of deterrence.[24] On the contrary, systematic *revision* poses a more serious challenge to international order. This occurs when technology empowers a state or a group of states that seeks to change the moral foundations of the existing international order.[25] Cyber power has

[22] The issues of attribution and offence dominance are discussed in Chapter Three of this study.

[23] Technological advances may strengthen certain states, move the system bipolarity to multipolarity or vice versa, encourage the creation of new norms, or enable new forms of conflict. In the present era, cyber power is causing systematic disruption altering the offence-defence balance, and weakening traditional security concepts such as deterrence and collective security (Kello, 2017, p. 89).

[24] Two examples of new deterrence concepts are “mosaic deterrence” (Buchanan, 2014) and “punctuated deterrence” (Kello, 2017, p. 205).

[25] For example, the 1930s saw development or refinement of technologies such as battle tanks, dive bombers, and aircraft carriers. These technologies, when organised using new operational concepts such as *blitzkrieg*, allowed Nazi Germany and Imperial Japan to inflict significant military defeats on their adversaries during the opening stages of World War II. If successful, these states would then have been able to impose their vision of systemic revision on the international system.

not brought about systematic revision, but Kello (2017, pp. 14-15) argues that it has empowered revisionist states (such as North Korea and Russia) that wish to challenge the existing liberal order.

More fundamentally, cyber space threatens to revise the system by creating a domain in which there is permanent hostility between the great powers. To date, there has never been a "cyber war"; all states have resisted the temptation to use cyber power in ways that would harm human beings in the physical domain. Nevertheless, cyber space cannot be characterised as "peaceful"; it is a domain of near-constant network intrusions, surveillance, economic espionage, and attacks by state-sponsored APTs. Kello (2017, p. 74) refers to this situation as "unpeace".

The most extreme form of technological disruption would be systemic *change*. This would occur if the power of non-state actors were to increase their power so substantially that the Westphalian system itself would cease to exist (Kello, 2017, p. 92). Clearly, we are far from such a transformation in reality, and in some respects, it is difficult to even imagine how a non-Westphalian order might emerge. However, Kello (2017, pp. 56-57) points out that in the cyber domain, non-state actors are able to wield relatively greater levels of power: corporations, criminals, militants, and hacktivists are all significant players. At the very least, this requires us to relax the assumption of methodological individualism in IR; it is simply not possible to assume that every cyber operation that emerges from a particular state was carried out with the consent of that state's government.

Kello does not argue that these changes are an inevitable consequence of the development of cyber space. Nevertheless, our theories must be able to *imagine* such changes, so that we have a benchmark with which to measure the real world. Most theories, he argues, can imagine only "instrumental instability": a situation in which states, locked in a familiar contest to advance their interests, make use of new and untested weapons (Kello, 2017, p. 119). This is a world of sub-optimal outcomes, but one that is explicable within the confines of rational choice theory. The danger, Kello (2017, p. 10) warns, is that cyber power may instead usher in a world of "fundamental instability": a chaotic world that empowers transnational actors and revisionist states, who then reject the international order or even the state system itself. Such a development may seem inexplicable from the perspective of traditional theories.

2.3 Constructivism: Norms and Securitisation in Cyber Space

The second major school of thought on cyber space and international politics is constructivism. In IR, "constructivism" is the newest of the major theories, having gained prominence since the 1990s.

Major proponents of constructivism include Kratochwil (1989), Onuf (1989), Wendt (1992, 1995, 1999), Ruggie (1998), and Finnemore and Sikkink (1998). In general, constructivists argue that the international system is socially constructed and should be understood as a system of social ideas, rather than a system of material capabilities (Hurd, 2008, p. 300).

Wendt's (1999) constructivist theory, which focuses on sovereign states as the unit of analysis, is arguably the most influential strand of constructivism in International Relations. In his approach, states are seen as almost analogous to people: they have identities and normative beliefs about right and wrong, are socialised by the international system, and assign social roles (such as "friend" or "enemy") to other states (Wendt, 2004). A key argument is that states do not have objective and eternal national interests; there is no "'portfolio' of interests that they carry around independent of social context" (Wendt, 1992, p. 398). Instead, a state's social identity *creates* its interests. This is not to say that material capabilities, such as the balance of military forces, are unimportant. However, material capabilities acquire meaning through the social ideas that are used to understand them. For example, Wendt (1995, p. 73) points out that five North Korean nuclear weapons would be seen as more threatening by the United States than 500 British nuclear weapons, due to the differing social context surrounding each phenomenon.

Wendt's theory tries to explain international outcomes in a holistic manner; like Waltz (1979), he is not especially interested in explaining the foreign policies of individual states. However, other constructivists have attempted to fill that gap; most notably, Finnemore and Sikkink (1998) in their research on the role of norms in bringing about change in international politics. In the view of Finnemore and Sikkink, norms are shared ("intersubjective") beliefs about what is right and wrong. Norms are social facts, and thus they cannot be observed directly, but their existence can be inferred from the restrained behaviour of powerful actors in the system.[26]

In this view of international relations, "power" can be understood as the ability to set and enforce norms, and "systemic change" can be understood as the transition from one set of prevailing norms to another. Finnemore and Sikkink (1998, p. 898) define a three-stage process through which international changes occur. First, there is a period of "norm emergence", in which "norm

[26] To illustrate this point, the United States has never signed the Ottawa Convention that bans the use of antipersonnel landmines. Despite this, it has not deployed these weapons since 1991 – even though it has fought unconventional conflicts such as the war in Afghanistan, where it might have gained some military utility from the area-denial capability of antipersonnel landmines (HRW, 2014). This suggests that the United States recognises (and largely accepts) the international norm against antipersonnel landmine use, even if it is unwilling to accept the specific legal requirements of the treaty which codifies that norm.

entrepreneurs" identify and champion a new norm. If they are successful, this triggers a "norm cascade", in which the new norm is adopted by states and formal institutions, and holdouts become increasingly isolated. Finally, this gives way to "norm internalisation", a steady state in which the norm is consolidated, violators are disciplined, and the new norm becomes settled wisdom.

In addition to the concept of norms, there is another concept from constructivist theory that is useful for understanding cyber space: securitisation. Securitisation theory is developed in detail by Buzan, Wæver, and Wilde (1998), all of whom are members of the "Copenhagen School" of security studies. In their view, "security threats" are social constructs and "securitisation" is the process through which they are constructed. They point out that all societies face constant challenges across many sectors: military, environmental, economic, social, and political (Buzan, 1991, p. 433). Some of these issues (but not others) are then defined as "security threats", effectively taking them outside the realm of normal politics and elevating to them to the status of a national interest. The securitisation of any particular issue over another is a performative act: "by saying the words, something is done" (Buzan *et al.,* 1998, p. 26). The overriding focus of the Copenhagen School has been to explain how and why certain issues are securitised and to ask whose interests are served by doing so.

Thus, there are at least two areas where a constructivist theoretical approach is potentially useful in understanding international cyber politics. An emphasis on securitisation raises the question: how and why has cyber space come to be defined as a security threat? And an emphasis on norms raises a somewhat different question: what are the prevailing norms on the use of cyber power in international relations?

2.3.1 The Cyber Securisation Theorists

In the first decade of the 2000s, a large number of scholars have discussed the internet through the lens of securitisation theory, arguing that the "threat discourse" which often surrounds cyber space is exaggerated and destructive. An early example of this school is Deibert (2003), who was one of the first scholars to question the then-dominant transnationalist school. Warning of the dangers of censorship and mass surveillance on the internet, Deibert (2003, p. 501) challenges the transnationalist view of the internet as an enabler of open global communication. Furthermore, in the aftermath of the 9/11 attacks, he argues that fears of cyber terrorism might lead to the militarisation of cyber space, and potentially draw the United States into a self-destructive cyber arms race against other countries (Deibert, 2003, pp. 517-518)

Nissenbaum and Hansen are among the first scholars to explicitly apply the securitisation framework of the Copenhagen School directly to the issue of cyber security. In an early paper on the subject, Nissenbaum (2005) argues that there are two competing conceptions of cyber security. The first conception is drawn from computer science, focuses on the protection of individual computers, and empowers individual security and privacy. The second conception is drawn from government agencies, focuses on the protection of national security, and empowers the state. Unfortunately, these two conceptions are in conflict with each other: attempts by government security agencies to increase their capabilities in cyber space have the effect of undermining individual security and privacy. This argument is extended in a follow-up article by Hansen and Nissenbaum (2009), which applies in more detail the framework of the Copenhagen School, and identifies a variety of official discourses surrounding "cyber threats".

Toward the end of the first decade of the 2000s, the broader debate over cyber space began to shift. The earlier transnationalist scholarship, which viewed cyber space predominantly as a source of power diffusion, was joined by a growing new realist discourse, which viewed cyber power as a tool for sovereign states to advance their interests. This was driven partially by real-world events, such as the absence of any serious cyber terrorist incidents, the revival of great power competition between the United States and Russia, and the Russian DDoS attacks against Estonia in 2008. It was also driven by the prominence of new authors, such as Clarke and Knake (2010).

Writing in this new intellectual context, Dunn Cavelty (2008, 2012, 2014, 2015) has arguably done more than any other scholar to apply securitisation theory to cyber space. She takes an explicitly constructivist view of the issue, drawing insights from both the Copenhagen School of Security Studies and combining these with theories of "framing" and "agenda setting" drawn from the discipline of media studies (Dunn Cavelty, 2008, pp. 25-33). Using these analytical tools, she traces the United States' official discourses on cyber security since the Reagan Administration, examining the ways in which discourses have evolved. In different periods of American history, different "cyber threat frames" have emerged. These have included: concerns over espionage during the late Cold War; concerns with "information warfare" and asymmetric conflict during the 1990s; and concerns over critical infrastructure protection after the 9/11 attacks. The underlying goal of all these threat frames, she suggests, is to justify the extension of American power into the cyber domain (Dunn Cavelty, 2015). They may also serve private interests; for instance, she argues that the most recent frame defines the cyber threat in relation to "business continuity". In this frame, corporate actors

become the referent object of cyber security, and threats to business are conflated with threats to national security (Dunn Cavelty, 2008, p. 137).

A similar line of reasoning is evident in the writing of Lawson (2013), who argues that the threat of cyber attacks has been heavily exaggerated in the United States. This rhetorical tendency is memorably described as the discourse of "cyber doom" (Lawson, Yeo, Yu, & Greene, 2016, p. 66). Evaluating this "cyber doom" narrative, Lawson (2013) argues that it is part of a long rhetorical tradition in which rapid technological change provokes fear and uncertainty. However, he argues that in the case of cyber security, such exaggerated fears are unrealistic and inhibit the formulation of effective public policy. Guitton (2013), who examines cyber threat discourses in Europe, makes a similar argument. He argues that the threat of cyber attacks on critical infrastructure has been heavily inflated, causing an overreaction from Germany, France and the United Kingdom. Ironically, he argues that this has resulted in resources being shifted away from efforts to combat the more prevalent (but less sensational) problem of cyber crime.

Overall, the securitisation theorists provide a critical perspective on official discourses surrounding cyber security. They correctly point out that extravagant claims about security threats should not simply be taken at face value. Instead, such claims should be examined carefully, especially when they are used to justify the expanding powers of agencies. However, the securitisation debate covers only one aspect of cyber politics. It was left to two other authors, Valeriano and Maness, to develop these insights into a broader constructivist theory of international cyber politics.

2.3.2 Valeriano and Maness: Cyber Regionalism & Restraint

Valeriano and Maness (2014, 2015, 2016) are the first authors to create a broad theory of cyber politics from an explicit constructivist perspective. Along with Kello (2017), Rid (2013, 2020), and Buchanan (2017a, 2020), they are also among the most systematic theorists of cyber politics and International Relations more generally. Their central contention, in common with many of the securitisation theorists described above, is that cyber threats are social constructs which have been exaggerated and overhyped. They are particularly critical of American political elites and intelligence practitioners, as well as certain transnationalist and realist writers (such as Kello and Clarke and Knake), who are seen as intellectual enablers of threat inflation (Valeriano & Maness, 2015, pp. 2-7).

Valeriano and Maness go beyond the securitisation theorists, combining this negative critique with positive empirical research on the dominant trends in cyber conflict. In their 2015 volume, they

develop a number of empirical claims. They argue that cyber conflict between states is relatively rare, and that cyber operations typically occur at a low intensity (Valeriano & Maness, 2015, p. 81). They find that the most common type of cyber operations in international conflict are DDoS attacks; as noted in Chapter One of this study, these block access to a website but do not allow the attacker to gain unauthorised access or compromise the integrity of a system (Valeriano & Maness, 2015, p. 34). They find that the majority of cyber attacks occur between regional rivals and that the majority of cyber incidents are examples of espionage, rather than destructive cyber attacks (Valeriano & Maness, 2015, p. 15). Finally, they find that cyber terrorism is almost non-existent and that terrorists use cyber space for recruitment and propaganda, not for carrying out attacks (Valeriano & Maness, 2014, p. 50).

Valeriano and Maness explain these findings by developing their own substantive theory of cyber politics, which is really a combination of two theories: a theory of cyber restraint, and a theory of cyber regionalism. The theory of cyber restraint argues that there are intrinsic features of cyber power that encourage states to use it sparingly (Valeriano & Maness, 2015, pp. 62-63). The most effective forms of malware rely on zero-day vulnerabilities.[27] Unfortunately for attackers, these are single-use weapons. After a zero-day has been exploited once, it is likely to be discovered and patched, reducing its effectiveness in the future. Such weapons can be used in surprise attacks, but not sustained international conflicts. Second, cyber weapons invite the possibility of blowback and escalation. If a state were to ever use any of the truly dangerous cyber weapons that are rumoured to exist (for example, logic bombs capable of disabling power grids), the conflict would quickly escalate into the kinetic domain and invite conventional military retaliation against the attacker. Third, cyber attacks create the potential for collateral damage. Like a biological weapon, computer malware can spread out of control, and might inadvertently harm the attacking state. And fourth, they argue that cyber weapons would inflict harm to civilians, thereby violating the most important norm of international conflict (Valeriano & Maness, 2015, pp. 62-63).

Valeriano and Maness (2015, p. 49) also propose a theory of cyber regionalism. They argue that international conflicts in the cyber domain usually occur between neighbouring countries, and typically involve disputes over territory. This is a somewhat counterintuitive view since it contradicts the commonly-held view of cyber space as shortening distance or even eliminating geographic

[27] See Chapter One for more information.

constraints altogether.[28] However, Valeriano and Maness (2015, p. 49) find that, even if cyber power gives states the hypothetical ability to launch attacks and engage in conflict behaviour with almost anyone throughout the world, they are unlikely to do so in practice unless they have a political objective they hope to achieve. For example, technology might give South Africa and Mongolia the ability to wage cyber warfare against each other, but they are unlikely to do so because they are far apart and have no incompatible interests to fight over. We can draw an analogy between cyber conflict and social media interaction: Facebook, WhatsApp, and similar platforms allow users to interact with almost anyone in the world, but most people use them to communicate with individuals they already know in person. Cyber conflict dynamics are similar, in the sense that they are more likely to arise within the context of long-standing territorial conflict (Valeriano & Maness, 2015, p. 74).[29]

Combining these two theories of regionalism and restraint, Valeriano and Maness (2015, p. 40) take a cumulative position they describe as "cyber moderation". They argue that cyber conflicts are likely to be rare; inflict only minor levels of damage when they do occur; to take place within regional conflict dyads; and be fought primarily over "traditional" territorial disputes. Their views on blowback notwithstanding, they are adamant that this relatively peaceful *status quo* depends on norms of self-restraint and *not* on deterrence through fear of retaliation (Valeriano & Maness, 2015, pp. 47-49). However, they also argue that the current situation is relatively fragile. If great powers, such as the United States, succumb to threat inflation, they might be driven by fear to implement policies that exacerbate the very threats they are trying to avoid. For example, if the United States constructs powerful offensive cyber capabilities and elaborate systems of deterrence, this will encourage other states to do the same thing. The correct course of action, they argue, is to strengthen nascent norms of self-restraint.

2.4 Realism: Bringing the State Back In

The third major school of thought is realism. Realist ideas began to permeate the study of cyber politics at roughly the same time as securitisation theory; like the securitisation theorists, realists tend to be critical of the expansive claims made by the transnationalist school.[30] However, their

[28] A typical example of this latter view is stated by Choucri (2012, p. 44), who describes cyber space as an arena that "transcends constraints of geography and physical location". See also Buchanan (2017a, p. 106).
[29] Examples of regional territorial conflicts that have been linked to cyber conflict include the disputes over Kashmir, the South China Sea, the West Bank, the Caucasus region, and Ukraine.
[30] Realists tend to be especially sceptical of the more radical transnationalists, such as Kello (2017), who argue that cyber power is a fundamentally transformative force in international relations.

underlying assumptions of realism are very different from those of constructivism. The central tenet of the realist school is that, even in the cyber domain, sovereign states remain the central actors. An important secondary tenet, following from the first, is the possibility of importing many of the traditional analytical tools that are used to study the broader world of international relations: anarchy, the security dilemma, deterrence, the offence-defence balance, and so on. In short, realists do not view cyber space as a separate political sphere, containing its own unique logic. Instead, they view cyber space as an extension of the existing international political realm.

The broader realist tradition in International Relations is a diverse one. It includes many sub-schools, classical, neo-, defensive, offensive, and neoclassical variants of realism. However, Wohlforth (2008, p. 133) argues that it is possible to identify four fundamental tenets that almost all realists would agree with. The first of these tenets is groupism: human beings must organise themselves into groups in order to thrive, and group solidarity at the international level is thus impossible to transcend. The second tenet is egoism: human beings are driven to seek out pleasure and avoid pain, which at the aggregate level translates into the pursuit of national self-interest. The third tenet is anarchy: there is no centralised authority at the global level, giving international politics its own peculiar set of attributes. The fourth tenet, which stems from the intersection of the previous three, is power politics: all human societies, across different historical epochs and geographic regions, tend to compete for political domination and resource control.

To what extent can this realist understanding of politics be applied to cyber space, a domain that seems to empower transnational actors and individuals (Eriksson & Giacomello, 2006, p. 229)? Some authors are sceptical of the value of realist approaches; Craig and Valeriano (2018, p. 95) argue that "realist theories about conflict often fall substantially short in explaining the unique dynamics of cyber conflict". However, other authors argue that it is necessary to use state-centric and geopolitical frameworks to understand cyber power. In one early example, Lonsdale (1999) argues that traditional geopolitical concerns will continue to shape politics in cyber space, while Rattray (2001) argues that "strategic information warfare" is a tool that states use to advance their national interests. More recently, Sheldon (2014) argues that physical geography still matters in cyber space, and suggests that regional geopolitical concerns continue to dominate in the realm of cyber security.

Several realist-inclined authors point out that internet traffic is carried over a physical layer of routers and servers, making it vulnerable to state control. For example, Goldsmith and Wu (2006) critique the "illusion" that the internet is a borderless international space. They argue that

governments still have the ability to enforce national laws in cyber space, and point to a number of cases where online actors have been successfully regulated or prosecuted. Deibert (2003) and Deibert and Rohozinski (2010) make a similar observation, pointing to the various strategies that states have used to assert themselves in the cyber domain. Governments have regulated key servers that act as "choke points", and coerced online companies by threatening their access to markets. In several cases, governments have used the internet to increase their power over societies, taking advantage of new opportunities for surveillance, monitoring, espionage, and control. For these reasons, Lake (2008, p. 50) argues that new communication technologies might serve to increase the relative power of states over transnational actors.

Like the transnationalist school described earlier, the realist position is not a unified one. The transnationalists, while relatively unified in their belief that cyber power is increasing the number of relevant actors, are uncertain about whether this development is positive. A similar divide can be seen among the realists. Starting from a realist framework, some authors assume that the likelihood of miscalculation and conflict between state actors is high. Others argue that the danger is low, and point out that "cyber power" fits easily into the familiar toolkit of statecraft instruments available to states; a position that is described in this chapter as "sceptical realism". In evaluating this school of thought, we begin by examining the work of Clarke and Knake, two authors that were among the first to bring the realist view of the cyber domain into the public consciousness.

2.4.1 Clarke & Knake: Cyber War and National Security

Richard Clarke is a security analyst and practitioner who served in the presidential administrations of Ronald Reagan, Bill Clinton, and George W. Bush. His perspective is therefore oriented towards policy analysis rather than the development of academic theories within International Relations, but his work nevertheless epitomises the early realist approach to the analysis of cyber politics.

In 2010, in conjunction with Knake, he published the book *Cyber War*, which helped bring the issue of cyber security to the attention of the public (Clarke & Knake, 2010). The book remains controversial; securitisation theorists in particular have attacked Clarke and Knake for their perceived alarmism (Valeriano & Maness, 2015, p. 10). Nevertheless, the authors make a number of important arguments. Their most important contention – which has since been accepted by nearly everyone – is that cyber insecurity is not merely a criminal justice problem, but is instead a potential threat to the security of states. Clarke and Knake (2010, p. 31) argue that a "cyber war" is a plausible future scenario, although such an event has yet to occur. They assert that physically destructive

cyber capabilities exist and claim that powerful states have already begun preparing the battlefield by placing logic bombs in each other's networks. In the most controversial section of the book, Clarke and Knake (2010, pp. 64-68) imagine a hypothetical cyber war scenario in which the United States suffers the complete collapse of its military networks, air traffic control systems, financial systems, and the electricity grid.[31]

What puts Clarke and Knake firmly in the realist tradition is their insistence that the most important actors are sovereign states. They downplay the risk of cyber terrorism, arguing that this is "largely a red herring", since terrorist groups lack the resources and skills to mount sophisticated cyber attacks (Clarke & Knake, 2010, p. 135). They are also surprisingly dismissive of the capabilities of multinational technology corporations. They are particularly harsh towards Microsoft; a company that, in their view, has created negative externalities by releasing buggy and vulnerable software (Clarke & Knake, 2010, p. 142). They argue that governments should take on a regulatory role in the provision of cyber security, enforcing common standards to ensure that corporations do not pass on the costs of insecurity to their customers. However, they lament this is unlikely to happen in the United States, due to the government's overly close relationship with big businesses and the pro-market ideologies of both of its major political parties (Clarke & Knake, 2010, p. 138).

Although Clarke and Knake assume that sovereign states in general are beneficiaries of cyber power, they argue that cyber power is weakening the relative position of the United States. They also argue that the strongest states in the system are also the most dependent on technology, and therefore most vulnerable (Clarke & Knake, 2010, pp. 148-150). By contrast, a less-advanced state such as North Korea has fewer technological dependencies and therefore presents a smaller attack surface to its adversaries. To put this in the language of International Relations theory, Clarke and Knake view cyber power as exerting a "balancing" rather than "bandwagoning" effect on the structure of the international system.

If this is true, however, then why has the United States not suffered a major cyber attack? One possible explanation, advanced by liberal transnationalists, is that the globalised economy creates complex linkages of interdependence that reduce the incentive for conflict. However, Clarke and Knake (2010, pp. 87-88) argue that this is incorrect – instead, they suggest that the global supply chains for consumer goods actually increases the likelihood of cyber conflict, since it creates multiple

[31] Valeriano and Maness (2015, p. 10) describe this section of the book as "a hyperbolic worst-case scenario". They also state that this scenario is "typical of the cyber hype industry" and is "troubling for many reasons".

entry points that can be used to insert malware.[32] Instead, they offer a simpler explanation for the lack of a major cyber war: states first "need to have the political circumstances that cause them to believe such an attack would be in their interest", and this situation has not yet occurred (Clarke & Knake, 2010, p. 67).

Interestingly, Clarke and Knake's (2019) follow-up volume, *The Fifth Domain*, adopts a somewhat more optimistic tone than their original book on cyber conflict. In this volume, the authors argue that more recent technological changes might have shifted the offence-defence balance in the cyber domain in ways that make a defensively oriented strategy more viable. They advocate for a policy program in which states deliberately attempt to shift the balance further toward defence by encouraging the development of more resilient networks and infrastructure. In doing so, they hope to increase the level of international stability in the cyber domain – a classic preoccupation of realist literature on international politics.

2.4.2 Rid, Lindsay, and Gartzke: The Sceptical Realists

A number of scholars responded to Clarke and Knake's argument by criticising its validity and arguing that cyber power is unlikely to have a transformative effect on international politics. These critics can be best understood as "sceptical realists"; Kello (2017, p. 3) refers to them as the "Clausewitzian" theorists of cyber conflict. These scholars tend to share Clarke and Knake's emphasis on sovereign states, as well as their view of cyber space as an arena in which states engage in competition. However, in contrast to Clarke and Knake (and Kello), these authors tend to argue that cyber power is a relatively limited tool that is unable to overcome the powerful tendencies toward continuity that exist in the international system.

J. R. Lindsay (2013, pp. 375-378) focuses on the Stuxnet malware attack against Iran, which is still one of the most dramatic examples of malicious computer software being used to attack a sovereign state. He argues that the Stuxnet case contradicts three expansive claims that are advanced in the transnationalist literature: that cyber power disproportionately benefits weak actors; that cyber power is offence dominant; and that cyber attacks are difficult to deter. In fact, J. R. Lindsay (2013, pp. 386-389) argues that the massive resources and institutional support required for Stuxnet suggest the opposite dynamic: cyber power enhances the capabilities of stronger states over weaker

[32] Since the publication of *Cyber War*, such concerns have become significantly more widespread, due in large part to the commercial success of Chinese technology companies such as Huawei and ZTE. See, for example, Finley (2019b) and J. A. Lewis (2018).

ones. Furthermore, despite the resources committed to it, Stuxnet inflicted limited damage against Iran, suggesting that the offensive potential of cyber power is small (J. R. Lindsay, 2013, pp. 389-397). Finally, J. R. Lindsay (2013, pp. 386-389) argues that both the original Stuxnet attack and retaliatory attacks by Iran show evidence of restraint, which suggests that even in the cyber domain, deterrence continues to exert a stabilising effect on international conflict.

Gartzke (2013) similarly emphasises the weaknesses and limitations of cyber power. Cyber power, he argues, should be understood through the lens of Clausewitz's dictum that warfare is a form of political action. When a state attacks another state, it does so with the aim of coercing its adversary or altering the balance of power in its favour (Gartzke, 2013, p. 42). However, the same feature that makes cyber power potentially destabilising – the possibility of states might carry out attacks anonymously, without attribution – also makes it coercively weak. To coerce an adversary, an actor must state demands and issue credible threats. In the cyber domain, however, the act of issuing a threat also serves to warn the adversary that his own systems are vulnerable and allows him to take action to avoid the danger (Gartzke, 2013, p. 56). For this reason, Gartzke (2013, p. 72) concludes that cyber power, though useful as a complement to other forms of statecraft, is ineffective as a policy instrument in its own right.

The most sophisticated and nuanced of the sceptical realists is Rid (2011, 2013). Rid, like Gartzke, grounds his argument in the military philosophy of Carl von Clausewitz. He argues that "war" should be defined narrowly, as political actions that involve at least the potential of violence against human beings (Rid, 2013, pp. 1-2). Violence, he argues, is the most distinctive feature of warfare – we cannot define non-violent action as "war" without diluting the concept to the point where it loses its meaning. However, by narrowing the definition of "cyber war" to actions in cyber space that create the potential for physical harm, we can impose analytical clarity on an otherwise-slippery concept. A consistent application of this definition suggests that cyber war is a purely hypothetical construct that has never occurred in the past and is unlikely to occur in the future (Rid, 2013, p. xiv).

This is not to say cyber power has no utility in international politics. On the contrary, Rid argues that there are three ways in which states can indeed use cyber power to advance their interests: by using the internet to sabotage, spy on, or subvert other states (Rid, 2013, p. 10). But these are merely technologically-updated versions of traditional tools of statecraft, which have been used by governments throughout history. Furthermore, Rid argues that cyber sabotage, espionage and subversion are limited in important ways, and are unlikely to have a transformative effect on

international politics (Rid, 2013, p. xv). Rid is fairly sanguine about the impact of such tools: he argues, provocatively, that the existence of non-violent policy instruments in the cyber domain is likely to reduce the overall level of violence in the international system (Rid, 2013, p. 166). Regardless, he argues, cyber power will not fundamentally alter either the existing balance of power or the state-dominated structure of the international system.

2.4.3 Segal and Klimburg: Strategic Culture in Cyber Space

During the 2010s, several real-world events occurred that seemed to validate the realist view of the primacy of states in cyber space. First came the revelation, in 2012, that the Stuxnet attack against Iran had been carried out by the United States. As J. R. Lindsay (2013) and Zetter (2014a) both point out, Stuxnet was an enormously complex and expensive weapon, which would have required significant investments in software development, testing, and supporting human intelligence. Then came Edward Snowden's 2013 revelation of the NSA's surveillance capabilities.[33] Together, these two events cast doubt on the transnationalist narrative, while strengthening the realist view. These events suggested that cyber power could be wielded most effectively by states – especially the great powers, which have the resources to develop cyber capability and the ruthlessness to use it.

In the aftermath of these developments, many scholars argued that states are now dominant actors in the cyber domain. Two notable examples of this trend are Segal (2016) and Klimburg (2017). Both authors are unenthusiastic about the trends they identify; they worry that attempts by governments to assert control over the internet could result in an increasingly fragmented and state-dominated internet, rather than the open and decentralised internet that was celebrated by the early transnationalists. In addition, both authors are notable for incorporating domestic political variables into their explanations of cyber politics. Other authors in the realist school have treated states as functionally undifferentiated units, differing in capability but pursuing essentially the same interests (Buchanan, 2017a, p. 19). By contrast, both Segal and Klimburg draw a distinction between states that support "digital sovereignty" (most of which are authoritarian), and states that are more supportive of an "open internet" (which tend to be democratic). Although neither author uses this terminology, their emphasis on unit variation and strategic culture essentially places them within the neoclassical realist school of thought in International Relations (Ripsman *et al*., 2016; Rose, 1998; Taliaferro, Lobell, & Ripsman, 2009).

[33] The surveillance operation revealed by Snowden was both massive in its reach and very expensive, suggesting that the NSA possesses capabilities and resources that far exceed those of any non-state actor (Lyon, 2014, p. 3).

For Segal (2016), the development of the internet has ushered in a new period in international politics that is comparable to the start of the Cold War. The key turning point in this "hacked world order" was the twelve months from June 2012 to June 2013, which Segal (2016, p. 2) refers to this as "year zero". This was the period in which Stuxnet was made public, Iranian hackers launched a cyber attack against the Saudi Aramco oil company, the United States repeatedly accused China of economic espionage, and the Edward Snowden leaks became known to the public.

Overall, Segal is focused on surveying the issues at stake – state hacking, surveillance, economic espionage, social media propaganda, and internet governance – rather than theory development. When Segal does engage in theorising, however, he tends to focus on strategic culture as a variable. States, he argues, do share broadly similar interests: all states want to protect their networks, grow their economies, and gather intelligence on their adversaries (Segal, 2016, p. 42). However, states vary in the precise way that they understand these interests. For example, states differ on whether "cyber threats" should be conceived narrowly, as technical attacks against networks, or broadly, as attacks against the social cohesion of a state. States also disagree over whether to focus their energies on internal or external threats, and whether to pursue growth in the technology sector through free markets, regulated markets, or strategic investment. Segal (2016, p. 41) describes these questions as the "cyber pachinko board" that collectively defines a state's strategic culture. He argues that each state's response to these dilemmas is likely to be "deeply rooted in [the] history, economics, and strategic challenges" of that particular state (Segal, 2016, p. 234).

Klimburg (2017) offers a more pessimistic account of security competition in cyber space. In his view, the freedom and openness of the internet is increasingly threatened by the rivalries between the great powers. States, he argues, have organised themselves into two informal coalitions, with each coalition articulating a different vision of how the internet should be governed. These two groupings engage in bipolar competition, a situation that Klimburg (2017, p. 109) explicitly likens to the Cold War. One coalition is organised around the concept of "cyber sovereignty", a belief that states should be free to apply their own domestic laws in cyber space. This grouping consists of mostly authoritarian states, and is led by Russia and China. It is opposed by a "free internet" coalition, consisting mostly of democracies, and led by the United States. The free internet coalition views the internet as a shared global space and, in principle, advocates for greater internet freedom. However, as Klimburg (2017, p. 360) notes, the United States' actions often fall short of its rhetoric, undermining its stated aims.

In Klimburg's view, the key arena in which this competition plays out is in the debate over "internet governance". Western democracies typically favour a "multistakeholder" model, in which the internet is managed by a combination of states, NGOs, individual technical experts, and private businesses (Klimburg, 2017, p. 106). By contrast, the "cyber sovereignty" coalition would prefer the internet to be governed by states alone, thereby allowing governments to exert greater control over the information their populations have access to. Klimburg is clearly liberal in his policy preferences – he strongly argues in favour of the multistakeholder model of governance – but realist in his analysis and predictions. The most likely danger emanating from cyber space, he argues, is not a catastrophic cyber war of the sort envisioned by Clarke and Knake in their 2009 volume. Rather, it is an insidious process in which the free internet coalition gradually compromises on its own ideals, the global internet becomes fragmented into national networks, and the internet increasingly becomes a tool for state control rather than freedom.

2.4.4 Buchanan: The Cyber Security Dilemma

The most sophisticated attempt to date to apply the realist theory of International Relations to the study of cyber politics are Buchanan's (2017, 2020) theories of the "cyber security dilemma" and "shaping and signalling". A key puzzle, for Buchanan, is to explain why states expend so much effort to break into each other's networks, even during peacetime. Would "cyber peace" not be more beneficial to all states? Buchanan finds that, while some of these actions might be explained by genuine aggression, states are also motivated by defensive considerations and foreign policy interests that that push them toward paradoxical outcomes.

The starting point for Buchanan's theory, as with all structural realist theories, is the problem of international anarchy. Since the international system is anarchic, and states cannot be confident that other states have good intentions, they develop military capabilities to protect themselves. However, this creates a security dilemma: as multiple states simultaneously build up military capabilities for defensive purposes, this paradoxically creates insecurity and magnifies the risk of war for everyone. Buchanan's innovation is to argue that the logic of the security dilemma also applies to conflict in the cyber domain, and that cyber conflict has certain intrinsic features that further exacerbate this dilemma.

Buchanan (2017) begins by noting that while cyber attacks can be executed rapidly, they are also complex, time-consuming, and slow to prepare. Once a state has decided to launch a cyber attack, the process of mapping the adversary's network and developing the necessary software exploits can

take months or even years (Buchanan, 2017a, p. 42). However, cyber operations are also characterised by a lack of momentum: states can go through most of these steps in advance, effectively taking them right up to the brink of conflict, without committing to the final decision to launch an attack (Buchanan, 2017a, p. 44). States can, therefore, speed up their cyber operations by preparing the ground in advance. In practice, this means hacking into other states' networks and establishing a persistent presence which can potentially be activated in the event of a conflict. Taken together, these dynamics create very strong incentives for states to launch persistent network intrusions, even during peacetime.

This "cyber security dilemma" is further amplified by the challenges of computer network defence. Due to the uncertainty and secrecy of cyber threats, states face the constant possibility that their networks have already been penetrated. To solve this problem, states may be tempted to launch "defensive" network intrusions: spying on their adversaries in order to determine whether they are being spied on themselves (Buchanan, 2017a, p. 65). However, if a state detects an intruder in its own network, it usually has no reliable way of gauging the intruder's intention. From the defender's perspective, it is difficult to tell whether an attacker is engaging in genuinely "defensive" espionage, or establishing a persistent presence as a form of contingency planning, or getting ready to launch an imminent cyber attack (Buchanan, 2017a, p. 76). If the defender chooses to adopt the worst-case interpretation, it may engage in retaliation and defensive intrusions of its own, further sharpening the cyber security dilemma.

In his follow-up book, Buchanan (2020) extends this argument and examines the operation of two other conflict dynamics that encourage the use of cyber operations: signalling and coercion. Buchanan argues that states have an ever-present need for tools that they can use to credibly signal their intentions and shape the incentives facing other states. In conjunction with the cyber security dilemma, this has resulted in a situation in which cyber operations have become a "new normal". Buchanan argues that cyber operations are more effective for coercion than for signalling. More broadly, his theories explain why cyber operations have become a pervasive feature of international politics during both peacetime and wartime.

Buchanan's achievement across these two books is his provision of an explanation for the prevalence of cyber conflict, operating irrespective of the intentions of individual states. He demonstrates that international anarchy, in combination with the intrinsic dynamics of cyber power, can result in an escalatory cycle of conflict – even when all states in the system have relatively

benign intentions. However, due to the “structural” character of his theories, Buchanan devotes relatively little attention to explaining the individual foreign policies of specific states. Like Waltz (1979, p. 72), whom he draws heavily from, Buchanan's primary aim is to develop a theory of international outcomes rather than a theory of foreign policy. By contrast, this study aims to build upon Buchanan's work by incorporating two new additions: exploring the reasons for variations in the cyber strategies of different states, and integrating both technical and persuasive cyber operations within a unified theoretical framework.

2.5 Other Perspectives

This chapter describes three broad schools of thought on international cyber politics: transnationalism, constructivism, and realism. However, there are several other perspectives that do not fit easily into this typology but are important and deserve consideration.

The first of these is neo-liberal institutionalism. Institutionalist perspectives in International Relations examine the ways in which states attempt to overcome collective action problems by forming institutions. Institutions are seen as facilitating cooperation by increasing the level of information available to states, discouraging cheating, creating opportunities for iterated bargaining, and lowering transaction costs (Keohane, 1982, 1984). At first glance, the liberal institutionalist perspective seems well-suited to addressing the problem of cyber security. All states would presumably benefit from greater levels of restraint and cooperation on cyber security issues. Several authors with diverse viewpoints, including Valeriano and Maness (2015, p. 205) and Clarke and Knake (2010, p. 254), have argued that an international convention on cyber conflict would be beneficial.

In practice, however, cyber security issues in international politics are only weakly institutionalised. The most prominent international treaty that deals with cyber security, the Budapest Convention on Cybercrime of 2001, has only 66 signatories and 63 state parties (COE, 2018). Craig and Valeriano (2018, p. 88) point out that “the cyber domain lacks effective global institutional governance... [r]elevant organisations include the International Telecommunications Union (ITU) and the Internet Corporation for Assigned Names and Numbers (ICANN), but their functions and competencies do not extend to conflict management”. As a result, cyber security seems to confound the expectations of liberal institutionalists; Drezner (2016) argues that “[i]nstitutionalists are hard-pressed to discuss the lack of cooperation in regulating cyberspace”. This can partially be explained by the technical difficulty of monitoring and verification of cyber security agreements, which poses unique (and

possibly insurmountable) challenges (Borghard & Lonergan, 2018). For now, it is fair to say that the cyber security landscape corresponds more closely with realist expectations than liberal institutionalist expectations.

Another perspective is that of international law. Several texts have sought to analyse cyber conflict through the lens of international legal theories, the most prominent of which are the Tallinn Manual (Schmitt, 2013) and Tallinn Manual 2.0 (Schmitt, 2017). These studies were commissioned by NATO and were co-authored by an international group of distinguished legal experts. They provide a comprehensive review of all existing international jurisprudence that is relevant to cyber conflict (T., 2017, p. 738). However, their interpretation of international law has been explicitly rejected by Russia and China, and is also not accepted as authoritative by NATO or its member states (Efrony & Shany, 2018). The ambiguous legal status of the Tallinn Manual and Tallinn Manual 2.0 is another indication of the weakly institutionalised nature of cyber security.

Finally, several scholars have considered ethical issues raised by cyber conflict, including the relationship between cyber conflict and Just War Theory. Dipert (2010) argues that Just War Theory cannot be used to analyse conflict in cyber space; by contrast, Cook (2010) argues that Just War Theory does indeed apply to cyber warfare, and that cyber conflict can be understood using analogies drawn from warfare in the physical world. Floridi and Taddeo (2014) provide an edited volume containing a large number of disparate viewpoints on the ethical problems inherent in cyber conflict. These sources provide an important normative perspective on cyber conflict; however, they are not directly relevant to this study, which focuses on the empirical determinants of cyber strategies rather than their normative dimensions.

2.6 Conclusion

This chapter identifies three broad schools of thought on cyber space and international politics: transnationalism, constructivism, and realism. Each school makes somewhat different assumptions regarding the principal actors, the most important variables, and the ways in which cyber space interacts with the international system. In general, the transnationalists tend to focus on power diffusion; the constructivists emphasise the importance of security discourses; the realists focus on power politics between states. However, this typology should not imply that each school is a single and unified grouping. In fact, there are significant disagreements within each of the major schools. Furthermore, not all these authors use these labels themselves. This schema attempts to impose a

structure on the theoretical debates within the sub-field, but it should not obscure the diversity of views on the topic.

The table in Figure 3 attempts to summarise some of the most important authors within each of the different schools. This table also includes the realist theory of cyber that is advanced in this study.

Scholars(s)	**Units of Analysis**	**Explanatory Variable(s)**	**Process**	**Dependent Variable(s)**
Arquilla & Ronfeldt	States; transnational actors	Technological & organisational advances	Networked organisation structures	"Netwars"
Liberal transnationalists	States; transnational actors	Technological advances	Economic interdependence & power diffusion	Reduced likelihood of war
Choucri	States; transnational actors	Technological advances	Lateral pressure	Cyber conflict and cooperation
Kello	Status quo states; revisionist states; transnational actors	Technological advances	Empowerment of revisionist states & non-state actors	Systemic disruption, revision, or change
Securitisation theorists	Socially constructed security threats	Threat discourses	Securitisation by security elites	Militarisation of cyber space
Valeriano & Maness	States	Norms & regional interests	Establishment of norms of restraint	Cyber restraint & cyber regionalism
Clarke & Knake	States	Technological advances	Miscalculation; aggression; over-confidence	Cyber conflict & cyber war
Sceptical realists	States	Pursuit of interests under anarchy	Moderate security competition	Continuity in the international system
Segal	Governments	Strategic culture	Security competition	State control of the internet
Klimburg	Governments	Regime type	Disagreement over internet governance	Bipolar conflict: "digital sovereignty" vs "free internet"
Buchanan	States	Anarchy	Security dilemma logic	Ubiquitous network intrusions
This study	States	Insecurity; institutional preferences	Erosion of trust in systems & institutions	Foreign policy strategy in cyber space

Figure 3: Summary of the most important authors discussed in this chapter.

Overall, it is evident that, since 1993, there has been an effort – halting, uncertain, but progressive nonetheless – to develop a theory of international politics in cyber space. Many of the earliest of these approaches now seem naïve and discordant with subsequent events. Arquilla and Ronfeldt, for example, foresaw the importance of networks but not, originally, of computers and software. The

liberal transnationalists of the 1990s took it for granted that greater access to information would increase the level of democracy and peace in the international system; they did not foresee the extent to which illiberal states would use cyber power to achieve their own foreign policy interests. Clarke and Knake, two early realist writers, worried about a catastrophic cyber war, and correctly predicted the development of weaponised malware such as Stuxnet and Flame. But they did not anticipate the more subtle and routine ways in which information would be made to serve the ends of states.

Over time, however, the sub-field has become more nuanced, more theoretically sophisticated, and more realistic in its treatment of technology. The sub-field has also lost much of its earlier innocence and optimism, and the most sophisticated proponents of each school now present a dark vision of the future. Kello's vision is one of aggressive revisionist states, using technology to engage in balancing behaviour against liberal democracies. Valeriano and Maness present an image of politicians and security agencies, distorting the benign effects of technology and stoking fears of international conflict. Finally, Buchanan presents states as being trapped in a tragic cyber security dilemma from which they are unable to escape, even if they have good intentions.

The theory developed in this study is situated within the broader realist school of thought on cyber politics. It focuses on states as the primary unit of analysis, and shares many underlying assumptions with authors such as Rid and Buchanan. However, it extends and expands on these arguments in several ways. Firstly, this study integrates both the technical and persuasive dimensions of cyber power into theoretical conception, which emphases the fact that all cyber operate by degrading and destroying trust in complex systems. Secondly, this study explores the reasons for variation in cyber strategies among states, seeking to explain the theoretical puzzle of why many states do not utilise the full range of potential cyber capabilities they possess. Finally, it tests this realist theory of cyber power by conducting three detailed case studies of specific states, evaluating them to determine whether they are congruent with this theory. The following chapter discusses this theory of cyber power in more depth.

Chapter 3
Theorising Cyber Power and Cyber Strategies

3.1 Introduction

On the morning of May 7, 2019, the city of Baltimore in the United States suffered a crippling cyber attack. The city's network was infected with a strain of ransomware called "RobbinHood", a type of malicious software designed to encrypt data and demand a ransom for its release. The attackers were not terrorists or a state-sponsored APT. They were, instead, petty criminals who demanded a payment in Bitcoin to reverse the damage they had caused. Nevertheless, the consequences of their attack were severe. When technicians shut down the network to prevent the infection from spreading, most municipal government functions ground to a halt. Citizens were unable to pay for services; the city's 10,000 employees could no longer communicate via email; the city's property market was suspended (Perlroth & Shane, 2019). Eventually, the situation was resolved, and the dust settled after what seemed to be just another instance of the growing problem of cyber crime. But then came an ironic twist: a *New York Times* report revealed that the exploit used in the attack, known as "EternalBlue", *had* been created by a state actor: the National Security Agency of the United States.[34]

How did an exploit developed by the American government and funded by American taxpayers come to be used against an American city? For years, US intelligence agencies such as the NSA had created exploits for popular software packages and used them to carry out espionage and sabotage operations against America's enemies. In 2013, a cache of these exploits was stolen by a mysterious group of hackers who called themselves the Shadow Brokers (Shane, Perlroth, & Sanger, 2017). The question of who the Shadow Brokers were and how they managed to steal the NSA's most valuable hacking tools has never been conclusively answered; one popular theory suggests that the Shadow Brokers were actually a Russian APT (Brandom, 2016). What is clear, however, is what happened next. Throughout 2016 and 2017, the Shadow Brokers repeatedly humiliated the NSA (and caused untold harm to the security of ordinary internet users) by publishing the exploits online. One of

[34] See Perlroth and Shane (2019) and Shane and Sreenivasan (2019). The NSA subsequently denied that EternalBlue was used in the attack (I. Duncan, 2019), but the *New York Times* stood by the original story, saying it was supported by "all four contractors hired to study the attack and restore computer services" (Shane & Perlroth, 2019). One security researcher has argued that the exploit used in the Baltimore attack may have actually been EternalChampion – a newer and more versatile NSA exploit, which was also leaked by the Shadow Brokers – rather than EternalBlue, as the *New York Times* reported (Root, 2019).

these was a potent exploit for Microsoft Windows, which the NSA had codenamed EternalBlue (Newman, 2018). Microsoft quickly patched the underlying vulnerability, but organisations that did not apply the patch remained vulnerable. In 2019, EternalBlue was downloaded by the criminal group RobbinHood, which used it to develop ransomware and extort money from a string of American municipal governments, including Baltimore (Chokshi, 2019). In its efforts to gain an advantage over America's enemies in the cyber domain, the NSA had inadvertently ended up supplying the tools for a cyber attack against one of the great port cities of the United States.

Two years later, halfway around the world, another state was forced to confront the costs of its aggressive cyber strategy. For years, the Russian government had used persuasive cyber operations to spread disinformation and viral conspiracy theories across social networks. These operations were part of a broader Russian strategy that sought to undermine institutional trust and spread discord amongst foreign societies. However, when the Covid-19 pandemic struck in 2020, it became clear that these disinformation campaigns had also created problems for Russia. Like many countries, Russia's response to Covid-19 was based on vaccination – in particular, its own homegrown Sputnik V vaccine. Sputnik V was the first registered Covid-19 vaccine, and while it was initially treated with scepticism in Western countries, clinical trials showed that it was safe and provided effective protection against the earlier variants of the virus (I. Jones & Roy, 2021). The Russian government took enormous pride in its rapid development of a Covid-19 vaccine, which it viewed as a demonstration of the country's technological prowess. Russia was quick to market the vaccine to other countries as part of a diplomatic strategy designed to increase its soft power (Vargina, 2020).

And yet, the Russian vaccine was met with high levels of distrust from the majority of Russians. The Russian populace, long exposed to government-propagated conspiracy theories, exhibited extreme levels of vaccine hesitancy. According to the 2021 Edelman Trust Barometer, Russia had the highest level of vaccine hesitancy of the 27 countries ranked in the survey, which significantly hindered the country's ability to control the pandemic and achieve herd immunity (Edelman, 2021). Distrust of doctors and the health system, online conspiracy theories, celebrity endorsements of misinformation, urban legends, and the declining quality of the health system all contributed to widespread hostility toward Sputnik V (Yablokov, 2021). Thus, the efforts of the Russian government to end the pandemic, restore economic normalcy, and create an appealing narrative about the success of Sputnik V were undermined by a culture of pervasive distrust that it was partially responsible for creating.

These two incidents, taking place in countries that are amongst the most enthusiastic users of cyber operations as a tool of foreign policy, demonstrate some of the costs and paradoxes that arise as a result. They serve as reminders that the cyber domain is fraught with unintended consequences and the ever-present possibility of blowback. This chapter explores these issues, attempting to understand the puzzle of why states would adopt policies that have the potential to harm their own national interests. It begins by making a conceptual distinction between "technical" and "persuasive" forms of cyber power. It then examines the main features of both types, including the conflict dynamics, incentives, and trade-offs that are associated with each. It argues that there is a fundamental similarity between the two forms and that both ultimately operate by undermining trust. However, neither form is cost-free: the aggressive use of cyber power in any form requires the initiating state to accept trade-offs to its economic welfare, its social cohesion, and its relationships with other states. Even in the cyber domain, states cannot simply do whatever they like. Instead, they must decide which of these trade-offs they are willing to accept.

This chapter aims to develop a theory about the types of states that are likely to accept particular combinations of trade-offs. Much of the previous literature on cyber strategy has relied on idiosyncratic or atheoretical explanations for these choices. For example, it is sometimes suggested that the unusual aspects of Russian foreign policy and cyber strategy under Vladimir Putin are influenced by the personal trauma that Putin experienced when he witnessed the collapse of the USSR from his vantage point as a KGB agent in East Germany and his determination to avoid a similar outcome in the future (Osnos, Remnick, & Yaffa, 2017). While this analysis probably contains a degree of truth, it is not especially useful to policymakers, since it does not give us insight into how other states might choose their own cyber strategies or help to understand how Russia's cyber strategy might evolve in the future. By contrast, this chapter argues that it is possible to develop a more parsimonious and useful explanation for cyber strategies by focusing on two primary variables: a state's external security requirements and its institutional preferences. By understanding these factors, we can explain and predict the cyber strategy that a particular state is likely to adopt.

3.2 Technical and Persuasive Cyber Power

When seeking to understand how cyber power is used in the context of foreign policy, a useful starting point is the conceptual framework developed by Rid (2013, p. 10). In this framework, offensive state actions in the cyber domain are grouped into three categories: "sabotage", "espionage", and "subversion". Buchanan (2020) makes use of a similar three-fold conceptual framework, distinguishing between "attack", "espionage", and "destabilisation".

Sabotage, in Rid's typology, is the most direct instrument in the cyber power toolkit. It involves the use of technical exploits, social engineering, and insider threats to penetrate an adversary's networks and disrupt complex technical or commercial systems (Rid, 2013, p. 57). In the language of the United States military, these types of operations are referred to as "Computer Network Attack" (CNA) operations. Sabotage is perhaps the most spectacular form of cyber power since the results are often clearly visible and can be felt directly by the victims. However, such operations are relatively rare.

A second, and far more common, type of cyber operation is cyber espionage (Rid, 2013, p. 81). In US military jargon, such operations are known as "Computer Network Exploitation" (CNE). In Russian military doctrine, by contrast, cyber espionage and sabotage threats are sometimes grouped together under the term "information-technical security" (Thomas, 2000, p. 345). Cyber espionage operations begin with the same steps that are taken in cases of sabotage: the use of exploits, social engineering, and insiders to gain access to adversary networks. The difference lies in the desired end state of the operation (Buchanan, 2017a, p. 76). A state carrying out a sabotage operation must expect that the operation will become known to the target at some future point, even if clever steps are taken to conceal it (Zetter, 2014a, p. 123). On the other hand, the end-state of a successful espionage operation is the continuous exfiltration of information to be used in other contexts (Rid, 2013, p. 82). In reality, of course, many espionage operations are eventually discovered. Notable examples include the malware "Agent.BTZ", which was discovered in US military networks, and the "GhostNet" malware, which infiltrated the offices of the Dalai Lama (Gamero-Garrido, 2014, pp. 20-21; Markoff, 2009). However, from the perspective of the state carrying out the espionage, the ideal situation would be the establishment of a presence in the adversary's network that remains in place forever.

The third type of operation identified by Rid (2013, p. 116) is subversion. In US military jargon, this sometimes goes by the rather sinister title of "psychological operations" or PSYOPs (Narula, 2004, pp. 178-179). In Russian military doctrine, these are described as "information-psychological" operations (Thomas, 2000, p. 345). According to Rid (2013, p. 116), the underlying goal of subversion is to undermine the strength of an established legal, political or social order. This definition identifies the key distinction that separates subversion from the two other forms of cyber power described above: it is social rather than technical in nature. Many forms of computer hacking use social engineering methods to gain access to an adversary's network, but subversive operations are unique in that they do not require the attacker to gain unauthorised access to computer networks at all.

They can be carried out in plain sight, using the exact same methods that are available to ordinary individuals – for example, by creating a user account and uploading content to Twitter, Facebook, or YouTube (Duncombe, 2017, p. 554). As a result, some scholars have argued that subversive operations should not really be considered a form of "cyber power" (Herrick, 2016). However, excluding subversion from this analysis would be to ignore one of the principal ways in which states pursue their interests within the cyber domain.

Nevertheless, it is clear that subversion is a very *different* sort of tool from sabotage and espionage. For this reason, this study groups sabotage and espionage together as "*technical*" tools of cyber power, in contrast with "*persuasive*" tools (see Figure 4). Technical cyber power allows states to advance their interests in the cyber domain directly; for example, by acquiring information that has strategic or economic value, or by sabotaging the efforts of an adversary. In its offensive form, technical cyber usually requires the use of some form of network intrusion to gain unauthorised access to an adversary's systems. On the contrary, persuasive cyber power operates indirectly. It seeks to influence the population of the targeted society to shape or constrain the foreign policy preferences of the state that is attached to that society. The extra step in the process means that persuasive cyber power is, in some respects, the more complex of the two tools. However, persuasive cyber power is also easier to use, in the sense that it does not require the attacker to gain unauthorised access to the adversary's networks. Persuasive cyber power is, by definition, exercised in the public view, although states making use of it often try to disguise the hand of the actor that lies behind it.

In some respects, the conceptual distinction between technical and persuasive cyber power maps onto Joseph Nye's classic distinction between "hard power" and "soft power". Nye (1990, p. 166) defines "hard power" as coercive; it tries to force compliance from other actors by threatening to destroy, harm, or impoverish them. In contrast, he defines "soft power" as attractive; it operates by persuading other actors to adjust their preferences voluntarily so that they are more in line with one's own (Nye, 1990, p. 167). In a later essay, Nye (2010) expands this broader framework into a typology of cyber power. Power in the cyber domain, he argues, can also be divided into "hard" or "soft" variants. Nye argues that a DDoS attack against a website would be an example of hard cyber power, whereas a "a public diplomacy campaign over the internet" would be an example of soft cyber power (Nye, 2010, p. 6). In addition to this distinction between hard and soft cyber power, Nye also makes distinctions based on the domain from which cyber power originates and the domain

against which it is directed, resulting in a typology of eight forms of cyber power in total (Nye, 2010, p. 5).

There are some problems with this framework, however. In addition to being rather complex, it is questionable whether all Nye's examples of "hard cyber power" are actually hard, in the sense of being coercive. This chapter argues that there are significant obstacles to the use of cyber instruments for coercion, unless they are used in concert with policy instruments in the physical domain (Jensen, Valeriano, & Maness, 2016; Valeriano, Jensen, & Maness, 2018). Furthermore, we might also question whether "soft cyber power" is really soft, in the sense of being attractive. Subversive cyber operations, as described by Rid (2013, p. 116) and Kello (2017, pp. 226-227) are often destructive rather than attractive in nature. They operate by breaking down the layers of epistemic trust on which human society depends. The value-laden term "soft" does not adequately capture the destructive logic of this form of power; for these reasons, this study instead uses the more neutral terms "technical" and "persuasive".

	Technical		**Persuasive**
Thomas Rid (2013)	"Sabotage"	"Espionage"	"Subversion"
Ben Buchanan (2020)	"Attack"	"Espionage"	"Destabilisation"
US military terminology	"CNA"	"CNE"	"PSYOPs"
Joseph Nye (2008)	"Hard cyber power"		"Soft cyber power"
Russian strategic doctrine	"Information-technical"		"Information-psychological"

Figure 4: Comparison of classification systems for cyber operations.

The remainder of this chapter delves into the features, trade-offs, and strategic logic that govern the use of technical and persuasive cyber power. Before considering these issues, however, it is necessary to examine a distinctive feature common to both types: the difficulty of attributing cyber operations to their source.

3.3 The Attribution Problem

In most cyber operations, the victim remains unaware of the attacker's identity. This phenomenon is known as the "attribution problem", and it is perhaps the most unusual feature of conflict in the cyber domain. Rid (2013, p. 141) observes that in all of recorded military history, there has never

been a major battle in which two armies fought without first identifying themselves. In the cyber domain, by contrast, concealment is the norm, and definitive identification is rare.

The attribution problem is a significant challenge for the defending side in both persuasive and technical cyber operations. As Rid (2013, p. 161) points out, there are really three attribution problems, which interact to produce great levels of uncertainty. The first of these is the problem of technical attribution: the forensic task of identifying the computer, network, or geographic region where a cyber operation originated. This is a tricky problem to solve, in part because of assumptions of good faith that were inherent in the original design of the internet (Clark, 2018, p. 194). As a result, identity signifiers such as IP addresses or domain names can be spoofed (Goutam, 2015, pp. 35-36), and attacks can also be routed through multiple stages to conceal the origin point of the attacker (Clark & Landau, 2011, p. 334). In the context of persuasive cyber operations, such as a disinformation campaign, the initiating state may employ tactics such as creating false accounts, and the use of existing social media networks as broadcasting channels. These tactics make it difficult for targeted states and security researchers to definitively trace the operation back to the source. If these technical barriers to identification are overcome, there is the additional problem of social attribution: establishing a relationship between a computer and the human operator who carried out the attack (Rid, 2013, p. 150). Even if this second attribution problem can be solved, there is still the final problem of political attribution: determining whether an attack launched from a particular territory was carried out with the support or consent of the country's government.

These conflict dynamics have important implications for deterrence in the cyber domain. In Albert Wohlstetter's (1958, p. 213) classic article on nuclear strategy, deterrence is defined as "a capability to strike second". Wohlstetter identifies a series of six hurdles that a state must cross in order to maintain deterrence: it must be able to survive an initial attack, preserve command and control over strategic forces, and so on. There is another hurdle that is left unstated, perhaps because it seemed too obvious to be worth mentioning: to respond to an attack, it is necessary to know who to retaliate against. It is relatively easy to determine the nationality of an invading army or the origin point of a missile trajectory. However, if a cyber attack cannot be attributed to its source, it will not be possible to retaliate. As such, many of the earlier sources on cyber conflict worried that cyber attacks would be difficult to deter, and this would create dangerous incentives for conflict and escalation in the cyber domain (Libicki, 2009, pp. 42-25).

In practice, however, we have not seen the general breakdown in deterrence or the widespread use of opportunistic cyber attacks that many analysts once feared. This probably stems, in part, from the fact that the attribution problem, while difficult to solve, is not insurmountable. In fact, cyber operations are often attributed with a fair degree of certainty. There are several technical approaches to solving the basic forensic problem, including aggressive methods such as "honeypots" and "hack back" tactics (Wheeler & Larsen, 2003, pp. 9-11). The United States' attribution of the Sony Pictures hack to North Korea, for example, relied on evidence collected by NSA intrusions that occurred at the time of the North Korea attack (Sanger & Fackler, 2015). More typically, the United States uses a combination of technical and non-technical methods to attribute cyber operations, including analysis of tradecraft, investigation of online infrastructure, and reverse engineering of malware (DNI, 2018). These attribution methods are not perfect, but they probably create enough fear of retaliation in the minds of potential attackers to ensure that there is still some deterrent effect in the cyber domain.

Private cyber security firms use similar methods of attribution, which serve as a useful resource for analysts (Romanosky & Boudreaux, 2019). In 2013, the security firm Mandiant released a ground-breaking report that analysed network intrusions against 150 organisations and attributed them to a single Chinese state actor. This was the first major case in which a private company was able to attribute APT activity to a state using evidence that could be examined by the public. Mandiant assigned the name "APT1" to the group, traced it back to the Pudong district of Shanghai, and concluded that it was actually Unit 61398 of the People's Liberation Army (Mandiant, 2013, p. 2). A similar example of private sector attribution occurred in 2016 when the security firm CrowdStrike attributed the DNC hack to the Russian APTs Fancy Bear and Cozy Bear (Alperovitch, 2016).[35] However, none of these findings was unequivocal. In each of these cases, well-informed sceptics within the security community have questioned the strength of these attribution claims (Sam Biddle, 2016; J. Carr, 2013; Krebs, 2017; Rogers, 2014; Schneier, 2015).

Political attribution is a common problem in the cyber domain, but it is not an entirely new problem in international politics. As Rid and Buchanan (2015, p. 4) note, the July Crisis that preceded World War I might be understood as a dispute over political attribution. The fact that Gavrilo Princip had killed Archduke Franz Ferdinand was not in dispute; the question was whether his actions could reasonably be attributed to the state of Serbia. This example serves to illustrate the significant

[35] Additional evidence in the DNC case was provided by another private security company, ThreatConnect (2016).

dangers that might arise from setting the threshold for political attribution too low. If attribution is inferred with too little evidence, states could be dragged into unwanted conflicts by the actions of rogue individuals within their borders. On the other hand, if the evidentiary threshold for attribution is set too high, this could also be destabilising. Governments would then be incentivised to carry out wanton cyber attacks, so long as they could use criminals or patriotic hackers[36] to establish a thin veneer of deniability. Unfortunately, there is no single rule or evidentiary standard that will provide the correct answer in every situation; the issue requires prudent decision-making on a case-by-case basis.

Since political attribution of cyber operations is difficult but not impossible, there is always a possibility that states that make use of aggressive cyber operations will experience retaliation, suffer unexpected blowback, or inadvertently encourage balancing behaviour by other states in the system. There are several ways in which states that feel threatened in the cyber domain might respond. Most obviously, a state that is the victim of a cyber attack might respond with a cyber attack of its own. Alternatively, states that are threatened in the cyber domain might choose to respond with kinetic military force. The United States (Sanger & Bumiller, 2011), the United Kingdom (Osborn, 2018), and NATO (2014) have all stated their willingness to escalate conflicts from the cyber domain to the kinetic domain. This option has an understandable appeal for states with powerful conventional forces, although it also creates obvious risks of escalation and unintended consequences. Most governments have been unwilling to state a precise redline that would cause them to escalate in this manner, but the general sentiment is conveyed in a quote from an anonymous US military official: “If you shut down our power grid, maybe we will throw a missile down one of your smokestacks” (Gorman & Barnes, 2011). In 2019, Israel announced that it had become the first country to put this doctrine into practice, launching an air strike in Gaza in response to an unspecified cyber operation by Hamas (Liptak, 2019).

States might also push back against hostile uses of cyber power by engaging in less risky soft-balancing tactics. “Soft balancing” is usually defined as the use of non-military tools (such as diplomacy, institutions, and economic statecraft) to “delay, frustrate, and undermine” adversaries (Pape, 2005, p. 10). Soft-balancing tactics are particularly useful for states facing cyber threats that do not justify resorting to war or retaliatory cyber attacks of their own. For example, during the early

[36] A “patriotic hacker” is an individual hacker who uses their skills to advance the interests of their nation and attack their country’s perceived enemies. States sometimes make use of patriotic to complicate the task of attribution or increase their leverage when using DDoS attacks.

years of the Obama Administration, the United States responded to Chinese economic espionage by publicising the hacks and trying to embarrass the Chinese government (Rogin, 2012). In the aftermath of the Edward Snowden leaks, China returned the favour by mobilising international outrage against the United States (helpfully deflecting attention away from China's own use of APTs in the process) (Farrell & Finnemore, 2013, p. 25). One variant of soft balancing is to construct coalitions of like-minded states to isolate adversaries, such as the Freedom Online Coalition (FOC), which generally supports the US stance on internet governance questions, and the opposing bloc of countries organised around 'digital sovereignty' that has been mobilised by Russia and China.

The key point here is that attribution is difficult but not impossible, which means that the exercise of cyber power is never without risk. Of course, this dynamic is not limited to (or even particularly acute within) the cyber domain; rather, it is something like a law of nature in international politics. For Brighi and Hill (2016, p. 149), all foreign policy decision-making is conditioned by the central strategic constraint that "even the most powerful actors might not be in the position to manipulate the environment around them fully". Realist thinkers such as Walt (1990, pp. 148-150), Pape (2005, p. 10), and Mearsheimer (2018, pp. 224-225) have all emphasised the tendency of states, when pushed by others, to push back in turn. Thus, it is not a new insight to suggest that states pursuing their goals more aggressively must accept a greater risk of resistance and retaliation. However, it is important to stress that the cyber domain is not, as is it sometimes imagined, a consequence-free zone in which great powers can simply do whatever they please. Balancing logic applies in the cyber domain, just as it does in other domains.

3.4 Features of Technical Cyber Power

The following section will investigate the conflict dynamics associated with technical cyber power. The goal of this discussion is to determine to what extent technical cyber power truly confers an advantage on the states that wield it and to identify the limitations surrounding its use. Three features of technical cyber power deserve particular consideration. First, its destructive potential remains largely unknown, not only because of the rapidly evolving nature of cyber technology but also because there has never been a true cyber war to date. Second, despite its theoretical potential to cause destruction, technical cyber power is coercively weak and often lacks the ability to compel adversaries to comply with demands or change their behaviour. In many respects, this is the flip side of the "attribution problem": states are reluctant to make concessions to an aggressor whose identity is unknown. Lastly, technical cyber power operates by exploiting vulnerabilities in networks used for commerce, communications, and military command-and-control. This is perhaps the most

important effect of technical cyber operations, as it allows states to directly degrade the capabilities of their adversaries by undermining their trust in technical systems.

3.4.1 Its Destructive Potential is Unknown

The first significant feature of technical cyber power is that there is a fundamental uncertainty over how much damage it can reasonably inflict. This uncertainty creates a challenge for security analysts and states alike, as they attempt to assess the true capabilities of cyber operations and the potential impact they may have on international relations. In the realm of warfare, the effectiveness of a weapon is often measured by the degree of damage it can inflict on an adversary. As Schelling (1966, p. 2) puts it: "the power to hurt is bargaining power". What "power to hurt" does technical cyber power possess?

In this regard, it is instructive to compare technical cyber power with other weapons that inflict pain on an adversary; for example, aerial bombing, blockades by warships, or nuclear weapons. Such weapons can be counted fairly easily, and their effects can be measured with weapons tests or inferred from previous conflicts (H. Kahn, 2017, p. 41). However, "cyber weapons" are really just software that is stored on computers. They are easy to conceal, and their effects are unknown until they are used. Fortunately, there has never been (and may never be) a true cyber war, as defined in Chapter One of this study. Until that threshold is reached, states will have strong incentives to keep their most powerful cyber capabilities hidden.

However, secrecy is only one part of the problem. There is also the more fundamental problem that the true destructive potential of cyber weapons may be unknown even to their creators. This is because malware is difficult to test in advance of deployment; it is also difficult to determine precisely how malware will behave once it is deployed on an adversary's network.[37] In some cases, a malware infection might spread more quickly than its creators intended;[38] in other cases, a software update or a small settings modification might suddenly render an existing cyber weapon ineffective (Hayden, 2016; Smeets, 2018, p. 14). In the face of such radical uncertainty, how should scholars

[37] See Nye (2017, p. 48). In the case of Stuxnet, American and Israeli planners appear to have solved this problem by building an elaborate replica of the Iranian enrichment facility at Natanz, using centrifuges obtained from Libya that were similar to the Iranian design (Zetter, 2014a, pp. 316-320). Despite this resource-intensive process development and bug testing, Stuxnet ultimately behaved in a way that was unintended by its creators: it spread into the wild, leading to its discovery by security researchers (Anderson, 2012).

[38] Examples of malware that spread faster than their creators anticipated include Stuxnet, as well the first major self-replicating worm in history, the Morris worm.

think about the effects of a possible future cyber conflict? It is important to avoid the unfounded fearmongering that Lawson (2013) describes as "cyber doom". However, we must also resist the fallacy that the philosopher Nassim Nicholas Taleb (2008, p. 56) describes as "naïve empiricism": the assumption that worst-case future scenarios are bounded by events that have occurred in the past.[39]

Instead, we can try to set plausible upper and lower bounds for the destructive potential of a possible future cyber war. The lower bound estimate is set by the intensity of cyber operations that have occurred in the real world; the things we know are possible because they have already happened. If this lower bound represents a real technical limit, then the worst that might happen in a cyber war would be more frequent incidents of the sort that have already occurred. These might include data breaches, the deletion of information in computer storage, and some limited sabotage operations with kinetic effects, but nothing comparable to the effects of conventional war. There is some evidence that such lower-bounded estimates may be accurate. For example, Barzashka (2013) argues that the Stuxnet cyber attack against Iran was an operational failure that inflicted little lasting damage against Iran, despite the extraordinary resources invested in its creation. If this is an accurate assessment of the most sophisticated malware attack in history, then we might be tempted to conclude that technical cyber power is simply a weak and ineffective weapon. This would also conveniently explain why no state has launched another cyber attack that is comparable to Stuxnet, despite more than a decade now having passed since Stuxnet was launched.

By contrast, an upper-bounded estimate proceeds from the assumption that *any* technological system can be compromised by a sufficiently dedicated adversary. The essence of this assumption is conveyed in an anonymous quotation that Segal (2016, p. 38) attributes to a member of the US intelligence community: "If you can imagine it, you can do it. It just takes time, money, and some effort." Several writers have tried to imagine conflict scenarios in which every technological system is vulnerable to cyber attack. Clarke and Knake (2010, pp. 64-68) speculate that even a limited cyber war might involve attacks on air traffic control, financial systems, and the electricity grid, resulting in thousands of casualties. In Singer and Cole's (2015) book *Ghost Fleet* – superficially a novel, but clearly intended as a scenario-building exercise for a cyber war[40] – the United States comes close to

[39] As Taleb (2013, p. 348) points out, this assumption has produced disastrous outcomes when applied in other settings. Examples of this fallacy are financial risk models that assume a bank is safe if it has enough cash reserves to withstand the worst financial crisis that has previously occurred, or military strategies that assume a state is secure if it can defend against the worst military attack it has faced in the past. When such risk models fail, the faulty assumptions that were inherent in the risk models usually seem obvious in retrospect. See Jorion (2000) for a case study of one such example in the area of finance.

[40] Unlike most novels, the book is sprinkled with academic citations.

losing a conventional war against China due to the crippling effects of cyber attacks against its military and civilian networks. Koppel (2015) sketches out a cyber war scenario that focuses on the loss of the electricity grid and the various second-order effects that this would have on public order, food security, emergency response, economic stability, and so on. All of these scenarios suggest that the potential damage from a high-intensity cyber war would be significant.

It is very difficult to estimate the likelihood of such scenarios, but there is at least some real-world evidence that they are plausible. The 2007 "Aurora test" revealed that it is possible to destroy components of an electrical grid using pure cyber methods (Srivastava *et al.,* 2013, pp. 236-237). "Nitro Zeus", an American cyber offensive against Iran that was planned (but never launched) after Stuxnet, was designed to disable Iranian power plants, communications, and air defences (Sanger & Mazzetti, 2016). Presumably, American military planners felt that this was a realistic reflection of their capabilities. A 2015 attack on electric substations in Ukraine caused temporary blackouts for 230,000 people, although power was restored six hours later (Zetter, 2016). In 2018, a Department of Homeland Security (DHS) report alleged that Russian APTs had penetrated US critical infrastructure networks, including "energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors", although the purpose of the intrusions was assumed to be reconnaissance rather than attack (DHS, 2018). And, in June 2019, the *New York Times* reported that the US had escalated its network intrusions into Russia's electric grid. This was described by US officials as a policy of "defending forward" to create a deterrent effect (Sanger & Perlroth, 2019).[41]

There are also persistent rumours of cyber weapons that would be even more damaging: logic bombs or "backdoors" hidden in critical infrastructure networks, perhaps at the hardware supply chain level. Such concerns appear to have motivated US efforts to blacklist the Chinese telecommunications manufacturer Huawei (Lecher & Brandom, 2019). The problem with such claims is that they are impossible to falsify; even if a system is audited and determined to be clean, it is always possible that the auditors did not look hard enough. However, security researchers have demonstrated that stealthy logic bombs are at least a theoretical possibility (Govil, Agrawal, & Tippenhauer, 2017). Overall, the evidence for the validity of upper-bounded assumptions is anecdotal and relies on investigative journalism and inferences from a limited number of cases; nevertheless, it suggests some cause for concern.

[41] The view that US intrusions into Russian critical infrastructure networks are "defensive" is, unsurprisingly, not shared by the Russian government.

3.4.2 It Is Coercively Weak

A second notable feature of technical cyber power is that it is not particularly useful for solving the basic foreign policy problem of coercing other states. At first glance, this might seem like a counterintuitive proposition. The preceding section has argued that the true destructive potential of technical cyber power is currently unknown, but potentially quite high. Furthermore, technical cyber power also has the unusual feature of allowing states to act without being definitively attributed, which may help to insulate attacking states against retaliation. In combination, these two factors might seem to make an appealing foreign policy tool for states that wish to coerce other states. In practice, however, any attempt at cyber coercion would face innumerable difficulties relating to signalling, commitment, principal-agent problems, incentives to avoid caving in to possible bluffs, and the inability of the attacking state to launch follow-up attacks.

Ironically, the fact that the same attribute that makes technical cyber power superficially appealing for many attackers – the difficulty of attributing attacks to their source – diminishes its effectiveness as a tool of coercion. As Gartzke (2013, p. 47) points out, coercion *requires* attribution: "[h]ow does one surrender to no one in particular?" We might refer to this problem as the coercion-attribution paradox. The paradox can be framed in the following general terms: an attacker can try to optimise a cyber attack to make it more coercive or more difficult to attribute, but any attempt to make a cyber attack stronger in one of these dimensions will probably make it weaker in the other dimension.[42] A related point is that cyber attacks that are heavily geared toward achieving a state's political interests should be less challenging to attribute since attribution can be inferred more easily from the motivations of the attacker (Rid, 2013, pp. 141-162).

To understand the limitations of technical cyber power, it may be helpful to consider a hypothetical scenario of cyber coercion in action. Rather than inventing a thought experiment from scratch, we can use a scenario that is helpfully provided by a 2015 Al Jazeera report, which suggested that Israel had threatened to launch a massive cyber attack against South Africa unless the latter agreed to modify its pro-Palestinian foreign policy (Jordan & Radhakrishnan, 2015). According to the news report, the South African government was allegedly given a 30-day window in which to end its support for the pro-Palestinian boycott, divestment, and sanctions movement. If it did not comply

[42] For more discussion of the relationship between coercion and attribution, see Betz (2012); Borghard and Lonergan (2017); Jensen *et al.* (2016); J. R. Lindsay (2013); J. R. Lindsay and Gartzke (2018); Valeriano *et al.* (2018).

with the ultimatum, it would suffer unspecified cyber attacks against its "banking and financial sector".

The source of the news report was a State Security Agency (SSA) intelligence document that had been leaked to *Al Jazeera*, as part of a series of embarrassing South African intelligence leaks that were dubbed "the spy cables" (Swisher, 2015). The conclusions drawn by the intelligence report seem dubious, however. In all likelihood, Israel never tried to coerce South Africa with cyber power (for reasons that will soon become apparent), and the so-called "former Mossad agent" who delivered the threat was a crank or a fraud.[43] Nevertheless, the scenario itself is an instructive one. Let us imagine a scenario in which Israel had, in fact, decided to use its technical cyber power to force South Africa to change its stance on the issue of Palestine. How might such a cyber conflict play out?

First, we should consider the relative strength of the parties. Israel is generally seen as being among the most capable states in the cyber domain (Valeriano & Maness, 2015, p. 26). It has an impressive IT security sector, good technical universities, and high levels of defence-related R&D expenditure (Tabansky, 2016, pp. 58-60). It controls a powerful signals intelligence (SIGINT) agency, Unit 8200 of the Israeli Defence Forces (IDF) (Reed, 2015). It has participated in at least two major offensive cyber operations: Operation Outside the Box, in which a cyber operation against Syria was used in combination with an air strike, and the Stuxnet cyber attack against Iran (Tabansky & Israel, 2015, pp. 65-67). By contrast, South Africa is at best a middle-ranking cyber power (Griffiths, 2017, pp. 55-61). A 2012 cyber power index, produced by Booz Allen Hamilton and the Economist Intelligence Unit, ranked South Africa at 16 out of 19 countries surveyed and awarded it a quantitative score of 30.2 points out of a possible 100 (EIU, 2012).[44] Such indices are simplifications of reality, but this nevertheless conveys a sense of the qualitative superiority enjoyed by Israel over South Africa in

[43] The *Al Jazeera* story contains several murky details that lead one to question the underlying story. The source of the threat was a hand-delivered note, sent from an "unknown source" to then-Finance Minister Pravin Gordhan in 2012. The author of the note claimed to be a former Israeli spy, and boasted that he had worked on the Stuxnet and Flame malware, but there is no evidence provided that he was telling the truth. The *Al Jazeera* reporters were careful to note that there is "no evidence that the threatened attack occurred or that the government yielded to the mysterious letter's demands", although many South African news outlets were less restrained when they repeated the story. The most plausible explanation for the reported sequence of events is that the "former Mossad agent" was lying. Another complication when assessing the story is that the SSA was heavily politicised during this period of South African political history, leading one to wonder whether its intelligence products from this era can be trusted; see J. Duncan (2014) and Pauw (2017) for more in-depth discussion of this phenomenon.

[44] Israel was unfortunately not one of the countries ranked, and so the index does not allow for a direct comparison of the two states.

terms of its technical cyber power. And yet, if Israel ever tried to use its cyber capabilities to coerce South Africa, it would probably find it impossible to do so. To understand why this would be the case, we can follow the sequence of probable moves and countermoves to its most likely conclusion.

The first problem for Israel would be to find a credible signalling mechanism to convey the threat. One option might be to make the demand through official channels, such as the Israeli Embassy. This would have the advantage of being an unambiguous signal, but it would also immediately sacrifice the main advantage that is usually enjoyed by the attacking party in the cyber domain: the uncertainty of attribution. A second option might be to convey the threat through an unofficial backchannel, such as the "ex-Mossad agent" in the SSA report. This would preserve some degree of plausible deniability, but there is a strong possibility that such a threat would be disbelieved and disregarded, resulting in the immediate failure of the attempted coercion.[45] A third option would be to communicate the threat through an anonymous channel, making attribution more difficult. However, this would be even less credible than a message delivered through an unofficial backchannel, and would also not be truly anonymous. There is really only one country in the world that has a strong interest in seeing South Africa abandon its support for BDS, and that country is, of course, Israel. Therefore, South Africa would suspect from the outset that the anonymous threat came from Israel, and this would greatly simplify the task of attribution.

After choosing a signal and the threat conveyed, the defender would now face the choice between capitulation and defiance. At this point, a second obstacle would confront the threatening state: the principal-agent problem.[46] In the *Al Jazeera* story, the cyber threat was levelled against South African financial companies, rather than the South African state itself. In theory, the South African state acts as an agent for the interests of South African society, including the private sector. However, their interests are not perfectly aligned: the immediate costs of capitulation (in the form of adjustments to foreign policy and increased vulnerability to future coercion) would be borne by the state, whereas the immediate costs of defiance would be borne by the private sector. This would make defiance a relatively low-cost strategy for the South African state. Even if the cyber threat were levelled against a government institution, it is likely that the ultimate cost of an attack (in the form of reduced service delivery) would be borne by the public rather than by the foreign policy executive directly. Such considerations might be partially counteracted by the state's long-term interest in the

[45] If the *Al Jazeera* report is taken at face value, this is exactly how South Africa responded after receiving the "hand-delivered note" in 2012.
[46] For a more generalised discussion of this problem, see Sappington (1991).

success of its national economy. However, realist IR theory (and real-world experience) suggests that states will usually accept some reduction of societal economic welfare if they believe that this is necessary to preserve their political autonomy in relation to other states in the system.

If this problem could be overcome, then Israel would face a third problem: conveying the credibility of the cyber threat itself. As this chapter notes, the precise effects of a cyber attack are difficult for either the attacker or the defender to predict in advance. In the face of such uncertainty, South Africa would have good reason to wonder whether the threat itself might be a bluff. Any state that suspects that it is being bluffed, even if it assigns a low probability to that possibility, has a strong incentive to remain defiant and call the bluff. This is because any state that signals a willingness to cave to possible bluffs will then expose itself to the possibility of endless blackmail from other actors in the future.[47] In our scenario, Israel might try to get around this problem by combining the original threat with some demonstration of technical capability and resolve. For example, it might decide to launch a more limited cyber attack as a precursor. If we assume the attribution problem has been solved at this point in the sequence, such a limited cyber attack would expose Israel to international censure. However, Israel would face a bigger problem: even a limited cyber attack would help South Africa identify and fix the vulnerability used to carry out the attack. As a result, it would be very difficult to carry out (or credibly threaten) a series of repeated attacks using the same set of methods.

Why would this be the case? As Chapter One of this study discusses, there are two main methods through which an attacker might gain access to an adversary's network: technical exploits and social engineering. Technical exploits can be further subdivided into two classes: zero-day exploits, which have never been used before, and previously-known vulnerabilities (Buchanan, 2017a, p. 107). With each of these attacking methods, any first use by the attacker will provide useful information to the defender that will help to protect them against future attacks.

The worst-case scenario for the defender is an attack that uses a zero-day exploit. Is this a realistic possibility in our scenario? In other words, does a state such as Israel possess zero-day exploits that

[47] In general, states are extremely reluctant to capitulate to threats that might later turn out to be a bluff. For instance, Saddam Hussein did not follow a policy of appeasement towards the United States during the Iraq disarmament crisis of the late 1990s and early 2000s, although in retrospect he probably should have. In 1998, the small state of Serbia refused to make concessions even when it was threatened by the combined might of NATO. From the Melian Dialogue onwards, history is replete with many other examples of weaker states that failed to make concessions to stronger powers in order to avoid war, even when it would have been rational for them to do so in the context of a non-iterated game (Blainey, 1988; Fearon, 1995).

would enable it to attack South African financial companies, if it wished to do so? Unfortunately, this is a difficult question to answer, because states have extremely strong incentives to conceal information about their stockpiles of zero-days. However, a 2017 RAND Corporation report provides a rare window into this secretive world. The report studied a team of sophisticated security researchers who focus on discovering new zero-days. The group was able to develop 207 exploits over a 14-year period; of these, 66 exploits were considered "living" at the end of the period (Ablon & Bogart, 2017, p. 14). The group is estimated by the authors to be on par with a mid-level state, and this gives us a very rough estimate of the size of a typical state stockpile (Ablon & Bogart, 2017, p. 11). Since even a single zero-day, if utilised effectively, can ensure the success of a cyber operation, a stockpile of 66 zero-days might seem to be very powerful (Zetter, 2014a, pp. 88-98). However, the subset of zero-days that are *useable* in any given operational context will be much smaller; in this particular scenario, we might speculate that the number will probably be in the order of single digits.[48]

In light of this information, we can now imagine how the final stage of the conflict scenario would play out. Let us assume that the defender has not capitulated, and the attacker is now faced with the decision of whether to press onward and launch the attack. In this scenario, we can assume that Israel has a stockpile of zero-day exploits that would enable the initial attack to succeed. However, zero-days are a rare and valuable resource. After the initial attack, the underlying vulnerability that enabled the exploit to work would be quickly identified.[49] In our scenario, South Africa would not even need to conduct this research itself; it could simply publicise the details of the attack and allow the worldwide community of private security researchers to discover and fix the vulnerability (Buchanan, 2016, p. 43). In the Stuxnet case, most of the defensive work was performed by private companies that were not directly employed by Iran, such as VirusBlokAda, Symantec, Kaspersky, and

[48] The operational requirements for a cyber operation are generally dictated by the software configuration and network topography of the target, and the attacker's pre-existing level of access. For a zero-day to work, there are two basic conditions that must be met: the target computer must be running the vulnerable software, and must be accessible to the attacker. In this scenario, we might assume that the target computers are running Microsoft Windows and are not physically accessible to the attacker. In the RAND dataset, only 69% of exploits affected Microsoft Windows, and only 50% allowed for remote execution (Ablon & Bogart, 2017, p. 47). However, there would certainly be additional operational restrictions layered on top of these, which would further reduce the number of zero-days available for use.

[49] It must be noted Stuxnet and Flame were able to operate in the wild for several years before being discovered by researchers. However, this was because of the elaborate precautions that were taken by the malware creators. Malware designed to coerce an adversary would have to create more obvious effects, which would greatly simplify the process of research and patch development.

Microsoft.[50] Thus, after the initial attack, we can expect that results would stand roughly as follows: the defender would have suffered significant harm, but the underlying vulnerability that enabled the initial attack would now be patched, the attacker would have lost some of its precious zero-days, and the opportunity for follow-up attacks would now be closed off. At this point, the defender would have very little reason to switch its strategy from defiance to capitulation. The attempt at cyber coercion would have failed.[51]

In the worst-case scenario for a defending state, in which an aggressor decides to actually carry out a large-scale cyber attack, the damage inflicted against the defender would mostly occur in the initial phase of the operation. Depending on the capabilities of the attacking state and whether we choose to assume an upper or lower-bounded estimate of the destructive capability of cyber warfare, the effects of such an attack can be quite severe – perhaps even comparable to a short air campaign. However, air campaigns have generally proven to be coercively weak, even when they are sustained over long periods and inflict massive levels of damage. If a state will not capitulate to an air campaign, it is unlikely that it would capitulate in the face of a comparatively short and non-repeatable cyber attack. Of course, such difficulties would be well understood in advance by any competent attacker; in large part, this explains why a scenario such as the one described previously has yet to occur in the real world.

3.4.3 It Undermines Trust in Technical Systems

The third notable feature of technical cyber power is that it undermines trust in technical systems. This helps to address an important theoretical puzzle: if technical cyber power is indeed coercively weak, as argued in this study, then why do states invest in it and utilise it? The answer is that, by

[50] In the Stuxnet case, this defensive effort required two main components: researching the malware, and deploying patches on the affected systems. Private research on the malware was conducted by Kaspersky (2015b); Symantec (2011); VirusBlokAda (2010) and Langner (2013). Microsoft's role was to develop and deploy patches to fix the vulnerabilities that were discovered, resulting in an unusual situation where a large American corporation was effectively helping to defend the Iranian nuclear programme against an American covert operation. For an in-depth discussion of the role of private security companies in discovering and defending against Stuxnet, see Zetter (2014a).

[51] We might ask: would the outcome be different if the attacker does not use a zero-day, and instead uses a previously known exploit? In that case, the result is even worse for the would-be coercer. After the initial attack, the defender would not need to allocate any time for researching the vulnerability or developing a patch; the patch would already exist. In such a scenario, the initial cyber attack would draw attention to the vulnerable system, and the system could then be patched. This is roughly the sequence of events that unfolded during the WannaCry infection of the British NHS, a real-world example of an attack that made use of a previously-known exploit rather than a zero-day (Hern, 2017). Most malware relies on previously known vulnerabilities; however, most malware infections are also opportunistic and are not targeted towards specific adversaries.

degrading an adversary's trust in their technical systems, a state can directly reduce the adversary's ability to achieve its foreign policy goals.

Trust is a fundamental component of human interaction and social organisation and plays a crucial role in various complex systems, whether they are technological, political, or economic. Trust arises from the interaction of formal security guarantees and informal social norms that create an expectation of security. It is the belief that others will act predictably and reliably without exploiting one's vulnerability. In modern societies, trust is essential for smooth functioning, enabling cooperation and reducing the need for constant vigilance against potential threats. Trust underpins commerce and business (Schneier, 2012). A buyer will be reluctant to enter their credit card information on a website, for example, if they do not trust that information to remain confidential. Over the longer term, trust reduces transaction costs in the economy, and is thus an important driver of economic growth (Fukuyama, 1996). In the political system, trust is associated with better provision of public goods, lower levels of corruption, and more effective democratic governance (Putnam, Leonardi, & Nanetti, 1994). In general, trust is an essential component in almost all modern economic, technological, and political systems (Rid, 2013, p. 21).

Trust also plays an important role in political decision-making, including decision-making in the realm of foreign policy. Foreign policy preferences are informed, at least partially, by their estimates of what is possible to achieve. These estimations, in turn, draw confidence from the technological and social systems used to carry out policies. To conduct ambitious foreign policy, governments must have confidence in the accuracy and reliability of the information and intelligence they receive, the privacy of their communications, and the technical systems that support their decision-making processes. For these reasons, the ability to undermine an adversary's trust in their technical systems can be a potentially useful foreign policy tool (Rid, 2013, p. 25). Fearon (1995, pp. 398-399), for example, points out that Japan likely would not have gone to war with Russia in 1904 if the government did not trust that its armed forces had at least an even chance of securing a favourable outcome.

The degradation of trust in technical systems is different from simple coercion. While coercion deters adversaries through fear of punishment, degradation of trust arises from an adversary's lack of confidence in their technical systems. This lack of confidence can lead to indecision, inaction, or misguided actions based on faulty information or systems, ultimately hampering their foreign policy objectives. Unlike coercion, which depends on clear signalling of intentions and capabilities, the

degradation of trust thrives on uncertainty. Both cyber attacks and espionage operations have the effect of undermining trust in this way.

For instance, Buchanan (2017a, p. 76) notes an intriguing aspect of espionage campaigns. Their objective is to avoid detection, and seemingly, the discovery of a cyber espionage operation implies the operation's failure. However, since it is impossible to prove a negative, the target will likely worry about the existence of other undiscovered espionage operations. Consequently, even the successful detection and removal of espionage operations may ultimately increase fear and uncertainty among policymakers. Moreover, as the initial stages of an espionage campaign are similar to those of a cyber attack, the target might worry about the potential for severe damage, especially if they adopt an upper-bounded estimate of the destructive capability of cyber warfare. Thus, even unsuccessful campaigns or cyber operations with dubious destructive potential can serve as effective signalling mechanisms.

By reducing the confidence that decision-makers have in their technical systems, it is theoretically possible for a state to alter the decision-making calculus of its adversaries. For example, a state might be inclined towards war if they expect that they are likely to succeed, and the expected benefits of the war outweigh the expected costs (Fearon, 1995). However, if the possibility of a cyber attack causes policymakers to doubt their ability to achieve strategic surprise or question whether their weapons will even work, their estimation of the likelihood of victory would decrease and the expected value of waging war would decrease. As such, even the possibility of a cyber attack might change the decision-making calculus of another state, shifting its preferences from war to negotiated bargaining.

Rid (2013, pp. 21-34) discusses two useful examples that illustrate how such conflict dynamics play out in practice. The first of these is Operation Outside the Box,[52] Israel's 2007 air attack against the Syrian nuclear reactor at Al Kibar (Harel & Benn, 2018). In 2007, Israel conducted a successful air attack against a Syrian nuclear reactor. The operation relied heavily on Israel's ability to disrupt Syria's air defence. By implanting malware within the Syrian radar systems, Israel effectively blinded them, allowing its non-stealthy aircraft to penetrate Syrian airspace and destroy the reactor (Fulghum & Wall, 2007). This operation not only destroyed a strategic target but also undermined trust in Syria's air defence systems, making the Syrian government more cautious and less capable of achieving its objectives. As a result, Syria was dissuaded from further attempts at nuclear

[52] Referred to in some sources as Operation Orchard.

proliferation. Rid (2013, p. 34) argued that the cyber component of the attack might have been more significant than the physical destruction of the reactor.

Another important example is the Stuxnet cyber attack against Iran, widely attributed to the United States and Israel, which targeted Iran's nuclear facilities, specifically the Natanz uranium enrichment plant (Sanger, 2012). The attack exploited vulnerabilities in the facility's industrial control systems, causing significant damage to the centrifuges used for uranium enrichment. This operation not only set back Iran's nuclear programme but also severely undermined trust in the technical systems underpinning it. The direct impact of Stuxnet on Iran's highly enriched uranium was relatively small (Barzashka, 2013). However, the operation appears to have undermined Iran's trust in its engineers and scientists and reduced confidence in its ability to protect its nuclear programme against future attacks (Sanger, 2012c). This cyber operation was part of a broader campaign of economics and coercive diplomacy that led to Iran's decision to sign the Joint Comprehensive Plan of Action in 2013.

3.4.4 The Trade-Offs of Technical Cyber Power

Technical cyber power has the effect of reducing trust in technical systems, creating fear and uncertainty in the minds of decision-makers about whether their technical systems they use to support their foreign policy goals will function as they intend. However, the use of technical cyber power to degrade an adversary's trust in this way has an important downside: it is almost impossible for governments to wield these tools without also inadvertently reducing trust in their own state's technical systems. This is because the internet is an interconnected global network – it is difficult to reduce trust in one part of the network without causing collateral damage in other parts of the network. As a result, states that choose to make aggressive use of technical cyber operations will have to accept a trade-off in terms of reduced network security.

This trade-off is particularly visible in two policy areas: the question of whether to disclose zero-day vulnerabilities and the question of how to handle encryption. Zero-days are the most powerful "cyber weapons", and they are extremely valuable for attacking states. A major reason for the success of the Stuxnet attack, for example, was its unprecedented use of four zero-days (Symantec, 2011, p. 25). However, zero-days are also rare, difficult to discover, and expensive to buy.[53]

[53] It is definitionally impossible to know how many unused zero-day exploits currently exist. It seems likely that they are rare; many thousands of software vulnerabilities are discovered each year, but only a very small percentage of these are ever turned into useable exploits. The assumption of zero-day rarity is supported by the high (and rising) cost of zero-days on grey markets where they are sold, with zero-days for Windows and

Furthermore, zero-days have a unique characteristic that differentiates them from all other weapons: once a zero-day becomes public knowledge, it is no longer a zero-day. Zero-day vulnerabilities that are revealed will be patched in about four months on average (Kenna Security, 2015), while vulnerabilities that are successfully concealed have an average life of about seven years (Ablon & Bogart, 2017, p. 52).

Thus, any state that discovers a new zero-day will have a strong incentive to conceal it in case it ever needs to use it against an adversary. However, it is always possible that some other actor will independently discover the same vulnerability. If a state chooses to keep the vulnerability a secret, its own civilian and commercial networks will be exposed to the same attack vector, potentially harming the attacking state's own economic interests. This policy is described by Zetter (2014a, p. 222) as "the equivalent of withholding a vaccination from an entire population so that a select few can be infected with a virus". Alternatively, a state can choose to disclose zero-days to software vendors, which will allow them to patch the vulnerability and increase the general level of trust in cyber security. However, the state will lose a potentially decisive instrument of cyber power. Thus, with respect to zero-days, it is logically impossible to maximise both technical cyber power and trust in network security: states must choose which goal they wish to prioritise.[54]

A similar dilemma emerges with the issue of encryption. Encryption is a key enabling technology that has helped to transform the internet from a collection of home pages into a viable tool for business and commerce. Without a reliable system of encrypting online communications users would be understandably reluctant to engage in commercial transactions or send confidential information over the internet. However, the widespread use of encryption has also created significant difficulties for intelligence agencies. Modern 256-bit public-key encryption systems, when implemented correctly, are effectively unbreakable at all plausible levels of computing power (Aumasson, 2017, p. 45). As a result, information sent over simple consumer-focused communication apps is sometimes impossible to intercept, even for state actors with access to vast computational resources.

WhatsApp fetching up to $1 million, and zero-days for iOS fetching up to $2 million (Goodin, 2019). For further discussion of the question of zero-day rarity see Grimes (2019).

[54] For more discussion on the dilemma posed by zero-days, see Ablon and Bogart (2017); Axelrod and Iliev (2014); Moore, Friedman, and Procaccia (2010). In practice, states can try to find ways to take a middle ground position. For example, the United States makes use of a formal "Vulnerabilities Equities Process" to determine which vulnerabilities should be disclosed and which should be stockpiled (EPIC, 2017). Even such middle ground policies will inevitably require sacrifices at the margins, however. For more discussion on the United States' policies, see Chapter Five of this study.

Some states view this as an unacceptable threat to their national security, and these states have engaged in a variety of attempts to weaken or regulate the use of encryption. The United States, for example, treated encryption software as a military technology before 1996 and prohibited American software companies from exporting it (Pasko, 2000, pp. 338-339). It eventually became clear that this policy was unworkable and it was abandoned; however, several Western countries, including the United Kingdom and the United States, have since tried to force smartphone manufacturers and online services to build "backdoors" into encryption schemes (Timberg & Miller, 2014; Whitehead, 2015). In 2018 Australia became the first liberal democracy to implement such a policy (Farivar, 2018). Computer security experts argue that the introduction of backdoors for law enforcement purposes will inevitably create technical weaknesses that will also be exploited by cyber criminals (O'Brien, 2018; Schneier, 2016b). Therefore, the regulation of encryption is another area in which states must choose whether to prioritise their technical cyber capabilities or trust in their domestic networks.

A lack of trust in network security can lead to businesses and consumers becoming hesitant to engage in online transactions, adversely affecting e-commerce and digital services. More broadly, the erosion of trust in the internet can have far-reaching consequences for the digital economy, the online dissemination of information, and the state's commercial interests. For example, China's reputation as an aggressive collector of online intelligence has created significant challenges for Chinese technology companies such as Huawei and TikTok. Huawei has been increasingly excluded from Western markets due to fears of Chinese intelligence infiltration (Salinas, 2018) and concerns over the high level of APT activity originating from China (FireEye, 2019). The blacklisting of Huawei by Western governments has resulted in its Android devices becoming less competitive in the US consumer market (Woo & Morris, 2018). The company has also been completely banned from selling network infrastructure in Australia (Finley, 2019a). More recently, the US government has banned the Chinese social media app TikTok on federal government-issued devices due to national security concerns over its parent company, ByteDance, and has contemplated a complete ban on the service for everyone in the United States (Bordelon, 2023). These examples demonstrate that technology firms may suffer significant harm and experience a loss of trust among consumers if their government engages in the aggressive use of technical cyber power. Even if a government does not prioritise the well-being of its citizens, this issue should still be a cause for concern. All states have an interest in maintaining economic growth, as the strength of a nation's economy serves as the foundation of its national power (Brooks, 1997; Mearsheimer, 2003).

It is important to note that this trade-off between trust and capability stems from logical incompatibilities between competing state interests in the cyber domain, and it cannot be avoided simply by allocating more resources towards the problem. For example, if a state discovers a new zero-day vulnerability, it *must* decide whether to disclose it or keep it secret. When making this decision, the state inevitably sacrifices either its offensive capability or network security. This trade-off cannot be circumvented by, for example, hiring more researchers and discovering more zero-days; in fact, this would only exacerbate the original dilemma. Ultimately, states that engage in aggressive cyber attacks, weaken encryption standards, and hoard software vulnerabilities will inevitably experience a decline in trust in their domestic networks, resulting in negative economic consequences. Different states make different choices about the severity of the trade-offs they are willing to accept.

3.5 Features of Persuasive Cyber Power

Having considered some of the most significant features of technical cyber power, we can now turn our attention to persuasive cyber power. Persuasive cyber power operates within a broader marketplace for information and ideas, shaping public opinion and decision-making processes. It exploits the social dynamics of homophily and memetic transmission, which enable the rapid spread and adoption of ideas among like-minded individuals and groups. The overall effect of persuasive cyber power is to undermine trust in institutions, making it a particularly useful tool for actors that wish to attack the institutional *status quo*. This section discusses the dynamics of persuasive cyber power and its impact on international relations.

3.5.1 It Operates Within a Broader Information Market

The first notable feature of persuasive cyber power is that it operates within a vast public space in which states must compete against millions of other voices. The internet can be conceptualised as a competitive marketplace for distributing information, in which ideas are debated, opinions are filtered, and preferences are formed. The online "information market" has three standard traits found in any economic market: producers, consumers, and competitive selection processes (Coiera, 2000). However, it differs from traditional markets in one important respect: it lacks producer scarcity. Unlike other commodities and services, information can be infinitely reproduced, with the marginal cost of supplying information to each additional consumer being effectively zero. This has encouraged many information suppliers to adopt a business model in which information is provided online for free, with users "paying" for information in the form of engagement (i.e. advertising

revenue) rather than currency. If we choose to model the internet as an information marketplace, then this raises several interesting theoretical questions. What are the long-term effects of disseminating information through competitive market mechanisms? Is the internet an efficient market, or does it suffer from inefficiencies and market failures?

There is an old and distinguished tradition in legal and political theory which assumes that information markets tend to be efficient over the long run, and that competition between ideas acts as a useful truth-selecting mechanism. The first clear expression of this view comes from the English poet John Milton (1918, p. 58), who suggests that we should simply "[l]et [Truth] and Falsehood grapple", since truth will always prevail in a "free and open encounter". Two centuries later, the utilitarian philosopher John Stuart Mill updated and refined this argument. Mill argues that truthful ideas have an inherent long-term advantage over falsehood: they can be successfully tested against reality. Thus, competitive information markets will eventually select ideas that are truthful, although the process may have to run through multiple iterations before this occurs: "The real advantage which truth has, consists in this, that when an opinion is true, it may be extinguished once, twice, or many times, but in the course of ages there will generally be found persons to rediscover it… until it has made such head as to withstand all subsequent attempts to suppress it" (Mill, 2017, p. 32).

The assumption that information markets are truth-selecting mechanisms has been influential in American jurisprudence and political theory. In his inaugural speech as president, Thomas Jefferson (2006) (whose party faced censorship and suppression under the Federalist administration of John Adams) argued that "error of opinion" should be "tolerated where reason is left free to combat it". In 1919, the renowned jurist Oliver Wendall Holmes (1919, p. 250) wrote a legal dissent in which he argued that "the best test of truth is the power of the thought to get itself accepted in the competition of the market". Justice W. O. Douglas (1951) agreed, arguing that "[w]hen ideas compete in the market for acceptance, full and free discussion exposes the false and they gain few adherents". This doctrine of the "marketplace of ideas" has been an important influence on the American legal understanding of free speech (Ingber, 1984, pp. 6-15).

Economic theory also gives reason to assume that a general increase in the amount of information available to citizens and consumers should have the effect of improving economic well-being. In the economic sphere, the most obvious advantage is the general reduction of transaction costs throughout the economy. The economists Ronald Coase (1937, 1960) and George Akerlof (1970) have pointed out that lack of information results in enormous hidden costs in all economies. In some

cases, buyers and sellers might simply be unable to find each other; in other cases, information asymmetries might make it impossible to determine who can be trusted, which in turn increases the cost of making and enforcing contracts. These transaction costs are difficult to see since they often take the form of potential opportunities that are never realised, rather than overt losses, but they nevertheless represent a significant reduction in societal welfare. It seems likely that many job openings have gone unfilled because employers and qualified candidates were unable to find each other; businesses that never got off the ground because entrepreneurs could not find reliable suppliers; the consumers who have entered into agreements with predatory firms because they were unaware of the firm's bad reputation; and so on.

The internet helps to reduce many of these transaction costs (World Bank, 2016, p. 42). There are numerous examples of information technologies being used to overcome transaction costs. Websites like Alibaba and Made-in-China.com allow even small entrepreneurs to establish international supply chains; LinkedIn connects employers with job-seekers; systems of "star rankings" on Uber or Google Maps help to reduce the reputational barriers that would otherwise discourage consumers from hailing a driver or trying out a new restaurant. Since the internet extends across international borders, this also means that innovative new business models which emerge in one country are quickly spread to new markets, through a process of transferral or imitation. Witness the speed with which media streaming platforms, ride-hailing services, and mobile payment systems have proliferated across the globe. This general reduction of transaction costs, and increase in innovation, is likely to benefit the interest of states by helping them grow their economies.

We might expect that a similar dynamic would also apply in the political sphere. As de Mesquita, Smith, Morrow, and Siverson (2005, p. 100) point out, democratic political systems can also be conceptualised as markets, in which political elites compete with each other to deliver beneficial policies to the "selectorate".[55] It is easy to imagine the existence of information-related transaction costs in the political arena that are analogous to those in economic markets: potential Pareto improvements that could be realised if information about individual preferences and the policy options for achieving those preferences were more readily available. Environmental policy and trade policy are two examples of policy areas that might be particularly susceptible to such problems. Both

[55] In the view of the authors, this process of competitive selection of public policy in democracies, however imperfect its operation, is responsible for the very strong correlation between political democracy and high quality of life. For detailed evidence of this correlation, see Frey and Al-Roumi (1999).

issues are notorious for pitting concentrated groups of winners against widely distributed groups of losers. Industries that pollute the environment, or are insulated against foreign competition, are strongly motivated to preserve the *status quo*; by contrast, the costs of pollution or reduced competition are spread evenly throughout society, so it is difficult to create well-organised coalitions to push for reform (Olson, 1965). If the internet increases the ability of affected individuals to coordinate or helps to disseminate policy options that would otherwise remain unknown, it might be expected to result in a higher quality of public policy overall.

And yet, it is difficult to say with any certainty whether the online "marketplace of ideas" has really enabled new public policies, and if so, whether this resulted in improvements to policy quality. Certain policies, such as Brexit or the Trump Administration's signature policy of building a border wall with Mexico, have arguably been enabled by online activism (T. Kaplan, 2019; Wutz & Nugteren, 2018). However, these were both controversial policies that did not result in clear Pareto improvements. It is possible that in the future, the internet will enable more effective policy responses to new collective action problems such as global climate change (Hestres & Hopke, 2017), but it is hardly certain that this will be the case.

Overall, the limitations of persuasive cyber power become evident when examining the competitive information market in which it operates. This is an environment in which states compete against numerous voices and a wide array of information sources. Furthermore, if state actors were to conduct persuasive cyber operations that attempt to twist the truth or promote propagandistic narratives, we might expect that competitive selection pressures would expose and counteract these false ideas. In practice, however, we can see that states have found ways to circumvent these challenges and effectively utilise persuasive cyber operations. They do this by exploiting inefficiencies and market failures in the online marketplace of ideas. These market failures include online echo chambers and filter bubbles, in which like-minded individuals reinforce each other's beliefs, as well as the fact that competitive information markets do not necessarily select for truthfulness. The following section will explore these market failures in more detail.

3.5.2 It Exploits Homophily and Memetic Transmission

In recent years, the traditional view of the "marketplace of ideas" as a truth-selecting mechanism has been subjected to sustained criticism.[56] In large part, this is because the normative ideal of rational and truth-selecting debate is so far removed from the real-world experience of using the internet. The internet is by far the largest, most competitive, and most democratic information market in human history; therefore, if information markets really operated according to truth-selecting logic, we could expect the internet to do a very good job of surfacing new and important truths. In practice, however, online information markets seem to have produced many undesirable consequences: low-quality "clickbait" journalism, outrage cycles, fake news, viral conspiracy theories, and so on.[57] The online political discourse that surrounds the news is even further removed from the rationalistic ideal and often consists of trolling, abuse, anger, in-group signalling, specious arguments, and motivated reasoning (Nagle, 2017; Vaidhyanathan, 2018). Persuasive cyber power operates by exploiting these failures in the information marketplace.

Why does this happen? As Coiera (2000, p. 219) points out, the unusual features of a market for information are responsible for creating many of these failures. Given the low marginal cost of replicating information, information producers have perverse incentives to focus on quantity rather than quality. Traditional journalism is expensive: for every publication like the *New York Times* or the *Wall Street Journal*, which conduct long-term investigations and maintain bureaus across the world, there are many more websites that specialise in creating high volumes of low-quality content, often merely recycling the day's headlines with an emotive and partisan spin.

In addition, the internet does not really function as a single, integrated information marketplace. Rather, it is a segregated marketplace that exhibits strong tendencies towards homophily. "Homophily" is a term used by sociologists, to describe the tendency of like to cluster together with like: "the principle that contact between similar people occurs at a higher rate than among dissimilar people" (McPherson, Smith-Lovin, & Cook, 2001, p. 416). In online political discussion, homophily is a self-sorting process, in which people are drawn towards online spaces that reflect their pre-existing views. Within each of these clusters, opinions are then subject to social reinforcement and

[56] See, for example, critical scholarship by Ingber (1984); Wonnell (1985); Kaufmann (2004); Wonnell (1985), and Joo (2014).

[57] A large body of recent scholarship in law, journalism, and media studies has investigated these problems. See for example R. L. Jones (2018); Napoli (2018); Hundley (2017); Waldman (2017), and Bybee and Jenkins (2019).

heresy-hunting dynamics that result in splintering and extremism. The result is a proliferation of insular, self-absorbed online political communities. Limberg and Barnes (2018) provide a fascinating taxonomy of the more notable political clusters that have proliferated in recent years, including "QAnoners", "Modern Neo-Marxists", "Social Justice Activists", "New Atheists", the "Dirtbag Left", the "Alt-Light", "Incels", and dozens of other groupings. In general, these subcultures tend to focus on reinforcing in-group beliefs rather than engaging in the competitive truth-selection process as envisaged by Mill.

Several studies have examined the phenomenon of online political homophily. Twitter has historically been a useful platform for this type of research due to the relative ease with which its social graph can be studied and mapped. Several studies of politically-active Twitter accounts in the United States have found that users do indeed self-organise according to party identification: both Democrats and Republicans are much more likely to follow and re-tweet their co-partisans (Colleoni, Rozza, & Arvidsson, 2014; Himelboim, McCreery, & Smith, 2013). The phenomenon has also been observed on Reddit, a platform where homophily is further reinforced through the mechanics of user voting (Mills, 2018). However, the most detailed study of homophily in American social networks has been carried out by Benkler, Faris, and Roberts (2018, pp. 45-74), who study the phenomenon across Twitter, Facebook, and the open web. Their findings suggest that the United States now possesses two separate media ecosystems: a left-wing/mainstream ecosystem, and an alternative/right-wing ecosystem. Americans have self-sorted into two online "content bubbles" that are almost completely disconnected from each other, and unable to achieve consensus over basic questions of fact.[58]

Homophily is an important dynamic, but there is another dynamic that is arguably more fundamental. Even if the internet did function as a single integrated market, it is not clear that it would select for truthful ideas. As Singer and Brooking (2018, p. 173) point out, the online "marketplace of ideas" is really a marketplace for human attention. In a situation where information is abundant, the human attention span becomes a scarce resource. These attention-seeking dynamics do not only select for ideas that are truthful or useful; they select for memetic transmissibility.

[58] One of the more interesting developments in the domestic politics in the United States over the last two decades is the way in which the internet seems to have undermined social cohesion, despite the United States possessing democratic political institutions which are explicitly designed to cope with such internal disagreement. This topic is explored in great detail by Benkler *et al*. (2018, pp. 45-74).

The term “meme” was coined by evolutionary biologist Richard Dawkins to describe the cultural counterparts of genes in evolutionary theory.[59] A meme is defined by Dawkins (2016, p. 249) as “a unit of cultural transmission”; examples of memes that he offers are “tunes, ideas, catch-phrases, clothes fashions, ways of making pots or of building arches”. Within this framework, ideologies and other complex belief systems can be thought of as collections of co-evolved memes that engage in strategic cooperation with each other. The defining feature of memes is they are replicators; they spread from one human brain to another through spoken language, traditional media, and the internet. Memes have a variety of secondary characteristics (for example, the type of emotion they excite in people who are exposed to the meme) that determine how likely they are to spread. Memes are not all created equal; some memes have stronger replicating tendencies than others, and these memes are thus more likely to survive and flourish online. One of the interesting features of memetics is its almost parasitic conception of the relationship between memes and their human hosts. Dawkins (2016, p. 255) argues that memes are “selfish”, in the sense that memetic selection favours attributes that are good for replication, rather than being good for the person who holds the meme.

Indeed, many of the strange and conspiratorial memes that exist on the internet have harmful effects on the individuals who hold them: they are associated with negative health consequences, interpersonal relationship problems, and social alienation (van Prooijen & Douglas, 2018, p. 899). For example, the “flat earth” meme is a fringe conspiracy, which alleges that the earth is flat and spreads primarily on YouTube; it leads to ridicule from broader society (Burdick, 2018). The “pizzagate” meme alleged that senior members of the Democratic Party, including Hillary Clinton and John Podesta, ran a child sex trafficking ring from the basement of the Comet Ping Pong pizza restaurant in Washington DC (Aisch, Huang, & Kang, 2016). One of the adherents of this theory, Edgar Maddison Welch, attempted to carry out an armed attack on the restaurant and received a four-year prison sentence as a result (Haag & Salam, 2017). The “anti-vaccination” meme, which has become particularly widespread in the aftermath of the Covid-19 pandemic, is perhaps the clearest example of a meme that is directly harmful to its host. It literally endangers the lives of its adherents and their children (Gould, 2017, p. 147). Nevertheless, all these memes have certain features that make them effective replicators, or they would not have been able to spread in the first place. For example, these memes might provide a sense of social validation (K. M. Douglas, Sutton, & Cichocka, 2017, p. 540), or a pleasurable sense of having access to special knowledge (Lantian, Muller, Nurra, &

[59] It should be noted that this study uses the term “meme” in the broad sense that Dawkins originally intended; not the narrower popular sense in which refers only to humorous images with text captions.

Douglas, 2017, p. 161). Whatever the reason, people who are "carriers" of such memes are sufficiently motivated to defend and advocate those memes online, thus spreading the meme to other internet users and repeating the cycle.

From a memetic perspective, persuasive cyber power can be understood as the ability of states to design, articulate, and spread memes that are beneficial to their national interests. For states that wish to make use of persuasive cyber, an obvious starting point is to determine the characteristics that make certain memes more likely to spread. Much of the research on memetic selection has been conducted by advertisers and marketing researchers, but the results are nevertheless quite illuminating for political scientists. Jonah Berger (2016, pp. 22-24) develops a set of criteria that he refers to as the "STEPPS" framework: "social currency, triggers, emotions, public, practical value and stories". Singer and Brooking (2018, p. 154) present a similar framework, which emphasises "narrative, emotion, authenticity, community, and inundation". The central contention of both frameworks is that memetic markets are *not* truth-selecting; rather, memetic success is heavily influenced by "non-rational" factors such as the social standing of the person spreading the meme and the type of emotions that the meme triggers. There is also strong evidence that people are more likely to accept memes that they are exposed to through existing social connections (Bughin, Doogan, & Vetvik, 2010). Studies on advertising have consistently found that people trust word of mouth recommendations over traditional forms of advertising (Nielsen, 2015). Similar attitudes exist towards political news. For example, a study of Russian public opinion found that "tips from friends" are overwhelmingly considered to be more trustworthy than other sources of information; they are trusted by 92% of respondents compared to 46% for traditional television advertising (Nisbet, 2015, p. 14).

There is also evidence that emotional impact and novelty are powerful drivers of memetic selection. Berger and Milkman (2012), in a study of online sharing of *New York Times* articles, found that articles that arouse strong emotions are more likely to be shared. Of the specific emotions coded into the study, "anger" was most strongly associated with selection (Berger & Milkman, 2012, p. 8).[60] Very similar findings are reported by Fan, Zhao, Chen, and Xu (2014), in a study of 70 million messages posted on Sina Weibo.[61] They, too, find that memetic markets tend to select for "anger" rather than competing emotions such as "sadness" or even "joy" (Fan *et al*., 2014, p. 5). One

[60] In this literature, anger is often described as a negative but "arousing" emotion. Berger and Milkman (2012) find that positive arousing emotions (such as awe) are also associated with online virality, although less strongly. "Deactivating" emotions, such as sadness, are negatively associated with online virality.
[61] Sina Weibo is a microblogging platform that is often described as the Chinese equivalent of Twitter.

particularly fascinating study, which examined 126,000 "information cascades" on Twitter, found that *falsity* is also a good predictor of success. News stories that were coded as being untrue were 70% more likely to be re-tweeted than genuine news (Vosoughi, Roy, & Aral, 2018, p. 359). Presumably, this does not mean that falsity is desirable in its own right; rather, this reflects the greater freedom that purveyors of fake news have to tailor their content to the specific emotional triggers described previously. By comparison, more traditional media organisations are bound by journalistic and ethical norms that make it more difficult for them to compete in the information marketplace.

There is a final point about memetic markets that is very important. Although it is possible to identify commonalities amongst the most popular memes, the selection process that determines which memes catch on and "go viral" contains a strong element of random chance and luck. One study, which attempted to study the spread of viral memes in real-time, found that "moderately popular [viral] events occur in our data at a rate of only about one in a thousand, whereas 'viral hits' appear at a rate closer to one in a million" (Goel, Anderson, Hofman, & Watts, 2015, p. 181). As such, even well-resourced actors such as sovereign states cannot simply order up a viral meme on demand; there is simply too much randomness and complexity in memetic markets. Nevertheless, states can and do try to produce memes with high transmissibility to increase their likelihood of success.

3.5.3 It Undermines Trust in Institutions

The third major feature of persuasive cyber operations is their tendency to undermine trust in institutions. Chapter One defines institutions broadly as the formal and informal "rules of the game" that structure human societies (North, 1991, p. 97). Institutions maintain political order, disseminate knowledge, and create a stable environment for cooperation and growth (Acemoglu & Robinson, 2012). In the context of international politics, institutions are typically created through international organisations such as the United Nations, NATO, the EU, and the World Trade Organisation (WTO). In the context of domestic politics, institutions include formal structures such as laws and constitutions, as well as informal norms and social practices.

However, Rauch (2018) points out that these political institutions are underpinned by epistemic institutions, which govern the production and distribution of knowledge. Epistemic institutions include academia, journalism, courts, the intelligence community, and all other professions that engage in hypothesis testing and knowledge production. These institutions play a vital role in

sophisticated technological societies, which are characterised by specialisation and division of labour. Due to the vast amounts of scientific and technical knowledge produced in such societies, individuals rely on these institutions to make informed choices as individuals and citizens. It is simply not possible for individuals to specialise in every academic field or to have first-hand knowledge about every subject needed to make decisions. As such, individuals must rely on their society's epistemic institutions to filter out unreliable information and provide reliable knowledge about topics that lie beyond their direct experiences.

Persuasive cyber power has a significant weakness: it struggles to effectively increase support for institutions. In politics, institutional trust emerges when governments consistently demonstrate trustworthy behaviour over prolonged periods (Putnam *et al.*, 1994). Similarly, trust in epistemic institutions arises through a pattern of reliable performance. For instance, a newspaper gains credibility by regularly publishing accurate stories, while scientific disciplines earn trust by consistently producing testable and accurate inferences. The scientific method has proven to be particularly effective in solving problems, which is why science is generally held in high regard. However, this trustworthiness is not achieved by chance. Epistemic institutions adhere to established rules such as peer review, replication of findings, confirmation and citation of sources, and enforcement of standards through professional bodies (Rauch, 2018). By following these rules, successful epistemic institutions accumulate a positive track record and win the trust of their audience over time. This level of established trust cannot be easily replicated through a persuasive campaign.

In principle, any actor – including a government agency – can create an account on a social media platform and attempt to persuade its audience to shift their views and preferences. However, without an established record or adherence to reliable epistemic rules, it is unlikely that such an actor would gain the trust of its audience. To illustrate this dynamic, consider a hypothetical scenario in which Russia wished to persuade European countries to leave the US-aligned NATO system and join its preferred security alliance, the Collective Security Treaty Organisation (CSTO). To achieve this goal, Russia might conduct a persuasive cyber campaign to convince Europeans that Russia and the CSTO would be trustworthy security partners. For example, the Russian state might create hundreds of thousands of accounts on various social media platforms, which would then be used to promote the CSTO as a reliable and trustworthy alternative to NATO. However, it is highly unlikely that this cyber campaign would have a significant effect on European public opinion. Europeans' trust in NATO stems from its 70-year history as a strong security alliance that has consistently maintained its

credibility through unequivocal security guarantees. On the contrary, many Europeans perceive Russia to be untrustworthy and would not have confidence in a Russian-sponsored security partnership such as the CSTO. A persuasive cyber campaign that simply asserted its trustworthiness on social networks would be unlikely to change this.

Alternatively, consider an alternative scenario in which the United States conducted a persuasive cyber campaign to convince audiences in African states to place greater trust in international economic institutions, such as the World Bank and the International Monetary Fund (IMF). Much like the hypothetical Russian campaign in support of the CSTO, this persuasive cyber campaign would likely fail. The distrust that many Africans feel towards the IMF and the World Bank stems from their negative experiences with the Structural Adjustment Programmes implemented in the 1980s and 1990s, concerns over the risk of debt dependency, and the perceived inability of these organisations to address poverty and promote economic development. It seems highly improbable that a persuasive cyber campaign would significantly alter these views. Even if the United States government were to create deceptive social media accounts that impersonate Africans, the target audience would probably not be influenced by the messages transmitted through these accounts, and if this deception were to be revealed it would then serve to heighten distrust in these institutions even further. Overall, these scenarios indicate that persuasive cyber power possesses an inherent limitation: it is an ineffective tool for creating trust where none exists.

However, persuasive cyber operations can be very effective at eroding trust. There are two primary reasons for this. Firstly, a state actor engaged in a disinformation campaign, unconcerned with promoting the truth or establishing trust, enjoys certain competitive advantages in the information marketplace. Such actors can generate destructive and conspiratorial memes that undermine trust in existing institutions without the need to demonstrate credibility or establish trust in the originating state (Farrell & Schneier, 2018). These narratives need only be plausible enough to sow doubt and uncertainty in the minds of the audience. Since it is unbound by the truth, such an actor can create narratives with high memetic transmissibility, deliberately evoking anger or tapping into pre-existing biases or social divisions. These false but emotionally triggering narratives can then be introduced into social networks. At each node in the network, they will be more likely to be reshared and replicated than truthful stories that lack similar emotional triggers. As this dynamic unfolds over multiple iterations, the network will gradually become inundated with false stories.

Secondly, even if these false narratives are exposed as being false in the competitive information marketplace, they can still contribute to the state actor's underlying goal of fostering cynicism, nihilism, and conspiratorial reasoning among its targeted audience. Indeed, if the audience of a persuasive cyber campaign realises that the information they are reading online is false, it may promote general cynicism about all information they encounter. Thus, there is a fundamental asymmetry between actors that are trust-based and those that are not. If an actor that relies on trust, such as a traditional newspaper or an academic journal, publishes information that turns out to be false, its reputation suffers, even if it takes steps to correct the problem. On the contrary, a state actor that seeks to undermine trust has little stake in its own reputation. If one of its social media accounts is exposed as a fake, it can simply create a new account and start broadcasting again. This problem was recognised by Saint Augustine more than 1,600 years ago when he warned his fellow Catholics against using lies to recruit potential converts: "When regard for truth has been broken down or even slightly weakened, all things will remain doubtful" (St. Augustine, 1952, p. 78). More recently, Steve Bannon, the former chief strategist for the Trump Administration, made a similar observation, albeit from a different perspective: "[t]he way to deal with [the media] is to flood the zone with shit" (Bannon, quoted in M. Lewis, 2018).

3.5.1 The Trade-Offs of Persuasive Cyber Power

Persuasive cyber power offers states the ability to influence and manipulate populations and undermines trust in targeted institutions. However, as is the case with technical cyber power, this carries important trade-offs. Most persuasive cyber operations are fundamentally deceptive. Some states do make use of overt public diplomacy campaigns; however, these do not appear to have had a particularly significant impact on international relations (Morozov, 2009a). By contrast, persuasive cyber operations have tended to have more impact when conducted covertly, using false online personas to conceal the state's involvement. Since the initiating state attempts to prevent attribution, it has more freedom to design untruthful narratives that spread more easily via a process of memetic transmission, sowing confusion and institutional distrust among the targeted population when these falsities are inevitably discovered.

The first trade-off is that any state engaging in duplicitous action suffers reputational risk, which can harm its ability to achieve its foreign policy goals in the future. For example, in the early 2010s, the United States carried out a fake polio vaccination campaign in Pakistan in its hunt for Osama bin Laden, secretly collecting DNA samples from Pakistani children. This fuelled public distrust of vaccinations in that country, which in turn hampered subsequent US-sponsored efforts to eradicate

the polio virus (Martinez-Bravo & Stegmann, 2019, p. 31). There is a similar dynamic at work in the cyber domain: once disinformation campaigns and other deceptive practices are revealed, the initiating state will be perceived as untrustworthy or hostile by other actors. The loss of credibility and trust can potentially have far-reaching consequences for a state's global standing, reducing its ability to cooperate on issues where there is potential for mutually beneficial bargaining and potentially triggering balancing and retaliatory measures from other states.

A second problem is that due to the interconnected nature of the global internet, persuasive cyber operations have the possibility of backfiring on the initiating state. This mirrors the problem seen with technical operations. Just as malware, once introduced into the wild, can end up infecting computers in the state that created it, so can attempts to erode trust within social networks end up damaging the initiating state's institutions and credibility. If disinformation campaigns and other persuasive cyber tactics are exposed, public trust in the epistemic institutions suffers. This is potentially a costly trade-off, since epistemic institutions such as the media, academic expertise, and trust in the government itself are important support structures for effective governance (Curran, 2005, pp. 120-137). These institutions help to promote informed decision-making, increased transparency and accountability, and encourage a more constructive discourse on public policy issues.[62] If trust in these institutions declines, this may hamper the state's ability to effectively govern and engage with its citizens. It is almost certainly not a coincidence that the citizens of Russia, a state that makes particularly intensive use of persuasive cyber power, have less trust in political and epistemic institutions than the citizens of any other country in the developed world (Edelman, 2022, p. 21; Sherlock, 2019).

Thirdly, states that aggressively employ persuasive cyber power may undermine their social cohesion, inadvertently harming their capacity to pursue ambitious foreign policy goals. Social cohesion, defined as the willingness of individuals to make sacrifices and cooperate in collective enterprises for the common good (Stanley, 2003, p. 8), is an important concept in the classical realist understanding of international relations. Notable realist thinkers such as Morgenthau (1993, pp. 117-122), E. H. Carr (2016, pp. 137-138), von Clausewitz (2008, p. 76) and Thucydides (2009, p. 39), have argued that political communities with high levels of in-group solidarity tend to have an advantage in international conflict.

[62] Voltmer (2010, p. 139) puts this point as follows: "[I]f citizens are ignorant about political issues, do not make an effort to have a say, despise their representatives, and do not believe in democratic values, the viability of that democracy might be seriously at risk — even if the institutions are perfectly designed."

In the neoclassical realist model of international relations, the state is conceptualised as an engine that extracts and mobilises the resources of society and redirects those resources towards its foreign policy goals (Taliaferro, 2006, pp. 485-487). Aggressive foreign policy strategies such as balancing or war are not only enormously expensive to implement but also compete with domestic priorities (Taliaferro *et al.,* 2009, p. 71). States with higher levels of internal trust and social cohesion will find it easier to mobilise popular support of such policies (Schweller, 2004, pp. 175-180). In contrast, an internally divided society increases the likelihood that interest groups within the state will attempt to withhold their resources or, in extreme cases, overthrow the state.[63] For this reason, Taliaferro (2006, p. 486) contends that a state's capacity for resource extraction and mobilisation will be severely limited if it suffers from "elite dissensus and fragmentation", and Schweller (2009, p. 233) argues that domestic unity is a necessary precondition for any aggressive or expansionist foreign policy strategy.

The trade-offs of persuasive cyber power, like those of technical cyber power, are not problems of resource allocation. Rather, they are logical trade-offs that stem from the inherent nature of the internet and human psychology. If a state introduces deceptive propaganda and misinformation into the social networks of its adversaries, allowing it to spread via a process of memetic transmission, it is technically challenging to prevent some of that misinformation from flowing back into its own social networks. It is an innate feature of human psychology that people, when lied to, will begin to doubt other purported sources of truth. There may be cases in which states deem these trade-offs worthwhile. However, as with technical cyber power, we should expect that states facing different strategic circumstances will make varying choices about which trade-offs they are willing to accept.

3.6 Explaining Cyber Strategy Selection

As we have seen, the exercise of both forms of cyber power requires states to accept significant costs and trade-offs. If a state aggressively employs cyber attacks and electronic espionage, it must accept some reduction in its domestic network security. If a state attempts to destabilise its adversaries through disinformation campaigns, it will very likely suffer costs to its domestic stock of institutional trust and social cohesion. Furthermore, since the attribution problem is not impossible to overcome, both forms of cyber power create a risk that other states will find ways to retaliate or

[63] Dissatisfaction with the high levels level of resource extraction required to fund aggressive foreign policy choices is a common feature of revolutions. The American Revolution of 1776, the French Revolution of 1789, the Russian Revolutions of 1905 and 1917, and the Iranian Revolution of 1979 were all preceded by periods of unusually high military expenditure and/or participation in expensive wars.

push back. These trade-offs can be somewhat blunted through clever workarounds or policy compromises, but they cannot be eliminated completely. As much as they might try, states cannot have everything their own way.

This brings us to the central issue of state strategy. In Chapter One of this study, cyber strategies are defined as patterns of behaviour in the cyber domain aimed at realising specific interests while navigating trade-offs between competing priorities. This definition draws inspiration from Luttwak's (2009, p. 409) conceptualisation of strategies as patterns of behaviour, as well as Porter's (1996, p. 70) observation that "strategy is choosing what not to do". As states grapple with the trade-offs of technical and persuasive cyber power and repeatedly decide which trade-offs they are willing to accept, certain patterns inevitably emerge. States weigh their interests, engage in iterated decision-making, set precedents that narrow the scope for future decisions, and gravitate towards particular sets of compromises. Some governments may prefer to specify and justify their chosen cyber strategy in written documents, such as the Cyber Security Strategy of the United States of America (2018). While these documents are useful resources for policy analysts and may hold value for the states that create them, it is crucial to note that strategies exist regardless of whether they are written down. In a sense, states cannot avoid having a strategy, as they cannot avoid making trade-offs in the cyber domain. A strategy may be inconsistent, ineffective, or incoherent, but it remains a strategy.

The core argument of this study is that states facing different strategic circumstances will make different strategic choices, and by understanding their circumstances, we can comprehend the choices states are likely to make. Given the trade-offs associated with both technical and persuasive cyber power, we should expect that the default approach for most states will be to use neither of these tools and instead adopt a strategy of restraint. This runs counter to some earlier studies on cyber conflict which assume there are strong systemic incentives for conflict in the cyber domain (Buchanan, 2017a; Clarke & Knake, 2010; Kello, 2017). However, this study hypothesises that there are two unit-level variables that encourage states to depart from this default strategy:

1. The first hypothesis is that states with high external security requirements are more likely to make aggressive use of technical cyber power. In this hypothesis, the external security requirement serves as the independent variable, while the state's use of technical cyber power functions as the dependent variable.

2. The second hypothesis posits that states with negative institutional preferences will aggressively use both technical and persuasive cyber power. In this hypothesis, institutional preferences are treated as the independent variable, while the state's use of persuasive cyber power is treated as the dependent variable.

Using arrow notation, the realist theory of cyber power presented in this study can be represented in a more simplified form:

- *Hypothesis #1: IV 1 (high external security requirement) positively influences → DV 1 (aggressive use of technical cyber power)*
- *Hypothesis #2: IV 2 (negative institutional preferences) influences → DV 2 (aggressive use of technical persuasive cyber power)*

The following sections discuss these hypotheses in more detail.

3.6.1 External Security Requirements

There are several reasons to expect that states with high external security requirements will be tempted to make aggressive use of technical cyber power. States that experience high security pressures are typically characterised by a combination of characteristics, such as geographic vulnerability, powerful and threatening rival states within their region, ongoing territorial disputes, and expansive foreign interests that require defence. There are several reasons to expect that such states will be more likely to develop and aggressively use technical cyber capability.

First, cyber operations serve as a cost-effective force multiplier that alleviates the issue of overstretch. Kennedy (1989) explains that expansionist states face continuous tension over whether to prioritise security spending or invest in economic growth. Powerful states often acquire far-flung economic interests, necessitating the protection of an ever-expanding military. However, investing too heavily in military security can result in armed forces growing beyond what the state's civilian economy can support. Brooks (1997, p. 446) describes this dilemma as one of "intertemporal trade-offs", a trade-off between present and future security interests. States with overstretched security requirements are likely to seek cost-effective, non-traditional tools to supplement their military capabilities in order to mitigate this trade-off. Cyber capabilities present a natural choice for such states, since cyber operations are often significantly cheaper compared to conventional military operations (Rustici, 2011, p. 34).

A second reason for security-conscious states to invest in technical cyber capabilities is to reduce the risk of strategic surprise. History is replete with examples of states that launch unexpected attacks against rivals in the hope of using the surprise as a force multiplier. Notable instances of strategic surprise include Nazi Germany's surprise attack against the Soviet Union in 1941 and the Japanese attack on Pearl Harbour in the same year (Betts, 1982, pp. 34, 42). More recently, the United States endured a psychologically devastating surprise attack on September 11, 2001, which led to two decades of costly conflict in Afghanistan and Iraq. Strategic surprise often has debilitating consequences for the states that experience it; therefore, states have strong incentives to mitigate this risk through continuous intelligence collection (Handel, 1984, p. 233). By investing in technical cyber capabilities, states worried about potential attacks can enhance their intelligence collection capabilities, potentially causing adversaries to doubt their ability to maintain secrecy and deter them from executing surprise attacks in the first place.

A third reason for the aggressive use of technical cyber power is to gain an advantage in bargaining or conflicts with other states. As several historical examples demonstrate, states with inside knowledge of the actions and decision-making processes of their rivals are more likely to achieve their foreign policy goals, both in peacetime and wartime. For instance, during the negotiation of the Washington Naval Treaty in 1921, the United States' "Black Chamber" SIGINT agency (the predecessor to the NSA) decoded communications between the Japanese delegation and their government in Tokyo, granting the US a significant negotiating advantage (Yardley, 1931, pp. 283-317). Two decades later, American SIGINT contributed to the destruction of the main Japanese carrier fleet during the Battle of Midway, which helped the United States win the war and emerge as the dominant power in the Pacific region (Keegan, 2004, pp. 211-252). These examples show that a state's security and relative power in the international system can be enhanced through intelligence collection, which can be further improved through the exploitation of communications technology. States facing abnormally high levels of international conflict therefore have an incentive to develop technical cyber capabilities to strengthen their position relative to other states.

Finally, a fourth reason to make use of technical cyber power is its potential as an effective signalling tool. Valeriano *et al.* (2018) argue that cyber power allows states to communicate displeasure towards adversaries without necessarily triggering further escalation. Through cyber operations, states can convey strategic messages to adversaries while minimising the potential for traditional armed conflict, thereby reducing the overall costs of signalling. However, the literature on signalling, such as Fearon (1997), suggests that inexpensive signals are generally less effective than costly ones,

meaning that the cost-effective nature of cyber power might work against it as a signalling method. Although this reason might be less significant than others, signalling intentions through cyber operations is nevertheless an additional tool that a state facing high security pressure can use to manage its external environment.

3.6.2 Institutional Preferences

As Chapter One discusses, states create international institutions to advance their interests and facilitate positive-sum bargaining. However, due to the range of possible bargaining outcomes over any international issue, it is unlikely that any given institutional order will be equally advantageous to all states (Fearon, 1995; Keohane, 1984). As such, we should expect that different states will adopt varying preferences regarding the institutional *status quo*.

Within a particular system, there are likely to be some states that benefit from the existing institutional *status quo* and wish to preserve it. These states are likely to have high levels of influence within existing institutions, either due to the way those institutions were designed or their historical role in creating them. Powerful states typically establish institutions when they are in a position of relative strength, thereby locking in their advantages and securing a disproportionately high share of the surplus gains from future bargaining (Gruber, 2000; Kindleberger, 1981; Krasner, 1985). Thus, these are likely to find that the institutional *status quo* offers them a stable framework for managing international relations that aligns with their goals and normative preferences. Such states can be described as having "positive" institutional preferences since their goal is to maintain and reinforce the existing institutional order.

However, if institutions are stacked in favour of the powerful, we should also expect that some other states will feel marginalised or disadvantaged by the institutional system. If the underlying balance of power shifts and these dissatisfied powers begin to rise, they will likely feel frustrated that the institutional *status quo* does not recognise their newfound status. Confronted with an institutional order they perceive as unfair, these states will then have strong incentives to try to revise it (Mearsheimer, 2018; Schweller, 2011). There are two logical ways in which this revisionism might be expressed.

Firstly, some states are likely to attempt to create and strengthen new parallel institutions that better align with their interests and normative preferences. The ultimate objective is to build, create, and strengthen a new set of institutions that they can control. Perhaps the clearest example of a

state in the current international system that has experimented with this strategy is the People's Republic of China, which has created many institutions such as the BRICS (Brazil, India, Russia, China, South Africa) group, the Shanghai Cooperation Organisation (SCO), the New Development Bank (NDB), the Asian Infrastructure Investment Bank (AIIB), and the Belt and Road Initiative (BRI). Although those following such an approach can fairly be described as revisionists, this revisionism is manifested in a "positive" way – creation as opposed to destruction.

In contrast, other states may adopt "negative" institutional preferences, and prioritise the goal of weakening or dismantling the existing institutional order. These states feel disadvantaged or threatened by the current system and believe that existing institutions do not serve their interests or cater to their normative preferences. Furthermore, they are sceptical of the possibility of creating a new institutional order that they could dominate. Thus, while these states are also institutional revisionists, they express their revisionism negatively. They might participate in the creation of new institutions to weaken the *status quo*, but their goal is not to create a new institutional order. Instead, their primary objective is to escape the constraints caused by existing institutions.

This study hypothesises that a state's preference for either strengthening or weakening institutions is an important determinant of its cyber strategy. To illustrate this logic, let us consider the decision-making processes of two hypothetical states: State P, which holds positive institutional preferences, and State N, which holds negative institutional preferences.

State P might be a *status quo* power, which benefits from the institutional existing order, or a revisionist power, seeking to challenge the existing order by establishing a new set of institutions. Either way, its goal is positive: it aims to increase trust in its own preferred institutions. State P might consider carrying out a persuasive cyber campaign to increase support for these institutions, but if it understands that persuasive cyber power is offence-dominant, it will realise that such a campaign will likely fail. An overt public diplomacy campaign would probably have little effect on its intended audience, and an aggressive disinformation campaign would tend to undercut institutional trust rather than increase it. Additionally, State P would likely recognise that a persuasive cyber campaign carries risks and trade-offs, including the possibility of potential blowback against their own domestic institutions and social cohesion. Given the low potential payoff and significant risks, there is a high probability that State P would rationally refrain from carrying out the operation.

On the contrary, State N holds negative institutional preferences and wishes to undermine existing institutions that it considers threatening or constraining. In this situation, the offence-dominant nature of persuasive cyber operations means that they would likely be quite useful for achieving this goal. State N could create narratives that weaken alliances and partnerships among adversaries, seed these into its adversaries' social networks, and allow them to spread through a process of memetic transmission. The existence of negative institutional preferences would not guarantee on their own that a state would choose to carry out the operation. The potential costs and trade-offs of the operation would still exist. However, compared to State P, the potential payoffs that State N would receive from carrying out the operation would be much larger. Therefore, if we assume that both states are rational actors motivated by self-interest, the probability that State N would choose to carry out the cyber operation is higher.

3.7 Four Ideal-Type Cyber Strategies

This chapter argues that there are two main types of cyber power: technical and persuasive. It hypothesises that states with high external security requirements are more likely to make aggressive use of technical cyber power, whilst states with negative institutional preferences are more likely to make aggressive use of persuasive cyber power. By plotting out these possibilities on a matrix diagram, we can identify four possible ideal-type strategies (see Figure 5).

The first strategy involves the restrained use of both technical and persuasive cyber power; this approach is referred to as a "restrained strategy" in subsequent chapters. This approach aims to maintain trust in a state's own networks and institutions. This study hypothesises that states will be more likely to adopt this strategy if they have low external security requirements and positive institutional preferences.

The second strategy involves the aggressive use of technical cyber power, combined with a restrained approach to persuasive cyber power. This is referred to as a "technical-aggressive" strategy in later chapters. In this strategy, a state seeks to degrade trust in an adversary's technical systems by employing offensive cyber operations and exploiting technical vulnerabilities. However, a state that adopts this strategy will exercise restraint in its use of persuasive cyber power and will typically refrain from carrying disinformation campaigns that undermine epistemic trust. This study hypothesises that this strategy is more likely to be adopted by states that are characterised by high external security requirements and positive institutional preferences.

The third possible strategy is a "persuasive-aggressive" strategy. A state that adopted this approach would seek to degrade trust in an adversary's political and epistemic institutions while exercising restraint in its use of technical cyber operations. This study hypothesises that a state would be inclined to adopt this strategy if it had both negative institutional preferences combined with low external security requirements. However, it seems unlikely that any real-world state would possess this particular combination of variables. A state with negative institutional preferences would, by definition, be placing itself in opposition to powerful states that benefit from the institutional *status quo*. A state in this position would almost certainly face high security pressures. Thus, while this strategy is a logical possibility within the confines of this model, this study tentatively hypothesises that we should not expect to see any real-world state adopting such a strategy.

		External Security Requirements	
		Low	High
Institutional Preferences	Positive	**"RESTRAINED STRATEGY"** Restrained use of technical cyber power Restrained use of persuasive cyber power	**"TECHNICAL-AGGRESSIVE STRATEGY"** Aggressive use of technical cyber power Restrained use of persuasive cyber power
	Negative	**"PERSUASIVE-AGGRESSIVE STRATEGY"** Restrained use of technical cyber power Aggressive use of persuasive cyber power	**"COMBINED-AGGRESSIVE STRATEGY"** Aggressive use of technical cyber power Aggressive use of persuasive cyber power

Figure 5: A typology of four ideal-type cyber strategies.

Finally, the fourth possible strategy involves the aggressive use of both technical and persuasive cyber power. This is referred to in subsequent chapters as a "combined-aggressive strategy". This strategy is a combination of the technical-aggressive and persuasive-aggressive approaches, focusing on both degrading trust in an adversary's technical systems and undermining trust in their political and epistemic institutions. It employs a wide range of cyber operations with the aim of weakening

the adversary on multiple fronts, disrupting their technical capabilities while also amplifying social divisions and decreasing trust in international institutions. This is a risky strategy, and this study hypothesises that it will only be adopted in the rare situation that a state has both high external security requirements and negative institutional preferences.

It is important to note that there are several limitations to this abstracted model. First, since these strategies are ideal-types, we should not expect any real-world state to perfectly conform to any one of them. In reality, state behaviour in the cyber domain exists on a continuum, with varying levels of aggression and restraint in the use of both technical and persuasive cyber power. This study does not claim that there is no variation with these four types of strategies; rather, the theoretical claim is that states leaning in one direction in one of the independent variables should lean in the same direction in the corresponding dependent variable.

Second, we need to make allowances for the role of complexity, chance, and emotion in human decision-making; therefore, we should not expect any real-world state to follow these strategies with perfect consistency in every situation. States may sometimes behave in unpredictable ways that deviate from the expectations of this model. Nevertheless, this study makes a theoretical claim that these four ideal-types follow logically from the trade-offs identified in this chapter. Over time, we should expect that all states which have the resources to carry out cyber operations will exhibit a probabilistic tendency towards one of these four strategies.

3.8 Conclusion

This chapter hypothesises that two key variables can explain a state's selection of its cyber strategy: external security requirements and institutional preferences. It suggests that states with high external security requirements are more likely to make aggressive use of technical cyber power, whereas states with negative institutional preferences are more likely to make aggressive use of persuasive cyber power. By extrapolating from these possibilities and mapping them out, we can identify four ideal-type cyber strategies: restrained, technical-aggressive, persuasive-aggressive, and combined-aggressive.

This chapter arrives at this conclusion through a process of deductive logic. Firstly, it develops a conceptual distinction between two policy tools that states employ to achieve their interests in the cyber domain: technical cyber power and persuasive cyber power. Technical cyber power encompasses cyber espionage and sabotage operations; it focuses on exploiting vulnerabilities in

technical systems. By contrast, persuasive cyber power aims to influence targeted audiences; it does so by taking advantage of market failures and inefficiencies in online information markets. Despite these operational differences, however, there is a fundamental similarity between them: both forms of cyber power work by undermining trust. Technical cyber operations compromise the adversary's trust in their technical systems, thus narrowing their range of foreign policy options. Persuasive cyber power, similarly, makes use of memetic transmission of ideas within an adversary's social networks to erode trust in their epistemic and political institutions.

Secondly, this chapter draws attention to the costs and trade-offs associated with both forms of cyber power. The core problem here is that the internet is borderless, which means that any attempt to degrade trust within another state has the potential to backfire on the initiating state. Additionally, the attribution problem is not insurmountable, which means that states on the receiving end of a technical or persuasive cyber operation may eventually identify the attacker and respond with balancing behaviour or targeted retaliation. As a result, states must make difficult choices about the forms of cyber power they wish to use. Over time, as states make repeated choices in the cyber domain, patterns will emerge, and we can identify the state's underlying cyber strategy.

This is the underlying logic for the realist theory of cyber power. A state is more likely to make aggressive use of technical cyber power if it faces high external security pressures that cannot be satisfied through conventional military spending. Furthermore, states with negative institutional preferences are more likely to make aggressive use of persuasive cyber power, since it offers them a higher potential payoff. A state that has both high external security requirements and negative institutional preferences is more likely to opt for a combined-aggressive strategy that employs both forms of cyber power.

Of course, this model abstracts from reality, and no state in the real world can be expected to fall perfectly into any of these categories. Despite these limitations, these four ideal-types provide a useful foundation for understanding and analysing state behaviour in cyberspace. By considering the strategies alongside the independent variables hypothesised to explain them, we can attempt to explain the broad contours of a state's cyber strategy. We can also make probabilistic predictions on how a state's cyber strategy would likely change if its underlying independent variables were to change.

The following chapters will attempt to apply and test this theory by analysing the actions of three different states in the cyber domain. Chapter Four considers the case of Brazil, a middle-ranking power with relatively low security requirements. Chapter Five investigates the United States, a powerful regional hegemon that nonetheless struggles to defend its expansive international interests. Finally, Chapter Six examines the cyber strategy of Russia, a revisionist state that aims to keep potential rivals off-balance and internally divided.

Chapter 4
Brazil

4.1 Introduction

This chapter examines the case of Brazil, attempting to analyse and explain its cyber strategy. Among the three cases examined in this study, Brazil is the least studied in previous literature on cyber politics. This is presumably because it is less interesting for many researchers. Although Brazil has developed significant technical cyber capabilities, it has consistently refrained from using them offensively. There is no evidence that Brazil has carried out destructive cyberattacks or engaged in intrusive espionage. Furthermore, Brazil has adopted a restrained approach to persuasive cyber power. It demonstrates considerable interest in internet governance and advancing its soft power, but it does not appear to have engaged in disinformation campaigns or seeded trust-eroding narratives in the information markets of other states.

The chapter begins by examining Brazil's restrained use of technical cyber power, discussing its development of potential technical cyber capabilities. It then discusses Brazil's approach to persuasive cyber power, focusing on its role in debates over internet governance and its apparent preference for maintaining trust in domestic information markets. It argues that Brazil has adopted a restrained approach in both areas, resulting in an overall strategy that approximates the "restrained" ideal-type discussed in Chapter Three.

For this reason, Brazil serves as a valuable negative case within the overall research design of this study. Sherlock Holmes famously solved one of his cases by identifying and explaining the absence of a phenomenon that would otherwise be expected to occur: a dog that does not bark at night (Doyle, 1894, p. 50). In the context of the cyber domain, Brazil is a non-barking dog: it is a state that almost certainly could make aggressive use of cyber operations if it wished, but chooses not to. This strategy of self-restraint is an intriguing theoretical puzzle that requires explanation. The Brazilian case is also useful for establishing a baseline standard of behaviour in the cyber domain, against which the more aggressive, risk-tolerant strategies of the United States and Russia may be usefully compared.

This chapter argues that Brazil's restrained cyber strategy can be explained by a combination of low external security pressures and positive institutional preferences. Brazil faces a secure regional environment due to a defensible geographical position, the absence of strong regional rivals and a

lack of major overseas commitments. Furthermore, Brazil's orientation towards international institutions is positive. It views institutions as useful tools to advance its national interests and its position of regional leadership and has generally prioritised the goals of creating, strengthening, and reforming institutions, rather than attempting to undermine institutions that it views as constraining. As such, the case of Brazil is congruent with the theory of cyber power developed in this study.

4.2 Brazil's Restrained Use of Technical Cyber Power

The most striking aspect of Brazil's approach to the technical cyber power strategy is its self-restraint. This restraint is not due to the absence of capability (Devanny, Goldoni, & Medeiros, 2022). Brazil is not a great power in the international system, but it is nonetheless a large, populous, and technologically sophisticated state.[64] It possesses well-funded security agencies, and it holds ambitious foreign policy preferences. As a result, Brazil almost certainly has the ability to use technical and persuasive cyber power if it wished, but it has refrained from doing so (Devanny *et al.,* 2022). This selection of trade-offs is a rational one for Brazilian policymakers to make. Due to its non-threatening international environment, Brazil faces relatively low external security pressures. An aggressive cyber strategy would offer limited payoffs while creating a serious risk of retaliation or blowback from other states. It is therefore quite sensible for Brazil to avoid such a strategy.

4.2.1 Building Up Potential Technical Cyber Capability

To demonstrate that Brazil has followed a policy of restraint in its use of technical cyber power, it is necessary to demonstrate that Brazil possesses significant potential technical capabilities, even if this potential has not yet been used. To this end, it is helpful to review Brazil's large and intricate set of cyber security agencies. The most important of these, in terms of resource allocation and offensive capability, is CDCiber, the Brazilian army's cyber defence unit (Diniz, Muggah, & Glenny, 2014, p. 3). However, Brazil also possesses many other organisations that focus on cyber security, which can be divided into three broad categories: internet governance institutions, incident response teams, and security agencies. The latter can be further subdivided into three main groups: military, intelligence, and policing.

[64] Using the definition of great power status articulated by Mearsheimer (2003, p. 4): a state with "sufficient military assets to put up a serious fight in an all-out conventional war against the most powerful state in the world".

Brazil's primary institution for internet governance is the Internet Steering Committee (CGI.br). This is a policymaking panel, originally created in 1995, with a mandate to promote infrastructure development, innovation, and internet access in Brazil (Segal, 2016, p. 205). It uses an innovative multistakeholder model.[65] It consists of 21 members, of which 9 are governmental representatives and 12 are non-governmental representatives (i.e. academics, NGO members, businesspeople, and technical experts) (CGI.br, n.d.). CGI.br also has an administrative arm, the Network Information Centre (NIC.br), which is tasked with managing and securing the ".br" top-level domain (NIC.br, n.d.). One of the interesting features of CGI.br is that it was established so early in the history of the internet; notably, it predates the creation of ICANN in the United States by two years (Almeida, Getschko, & Afonso, 2015, p. 76). Through this agency, Brazil has created a model of internet governance that is widely admired across other states (van der Spuy, 2017, p. 44).

Brazil also possesses a large number of incident response teams (or "CSIRTs") that are spread out across its largest provinces and major cities. These teams would constitute the front-line response in the event of a major cyber security incident. One such team is CTIR.gov, the Brazilian federal government's own CSIRT, which is tasked with securing government networks (CTIR.Gov, n.d.). To coordinate this and other teams, NIC.br maintains a National Computer Emergency Response Team (CERT.br.), which acts as an umbrella CSIRT for the entire country (CERT.br, n.d.). One possible weakness of this system is the large number of incident response teams; M. G. da Silva (2019, p. 15) provides a list of 40 different governmental CSIRTs across Brazil, in addition to CERT.br and CTIR.gov. In the event of a major cyber attack, the coordination of these various CSIRTs would probably constitute a significant organisational challenge.

In addition to these governance and incident response groups, Brazil also has a constellation of security agencies that focus on cyber issues. Brazil is somewhat unusual among democracies in that the military (in the form of the Brazilian Army) has assumed a leading role as a provider of cyber security for civilian and military networks. The Army's role began in 2008, with the publication of Brazil's National Defence Strategy. This document defines three "strategic sectors" as being vital for Brazil's future national security: space, nuclear, and the cyber domain (Brazil, 2008, p. 32). In 2012, the government published a White Paper on National Defence, which develops these strategic themes in more detail (Brazil, 2012, pp. 71-72). These policies led to the creation of Brazil's most

[65] "Multistakeholderism" is a model of internet governance in which governments cooperate with non-governmental groups (including private business, civil society, academic researchers, and technical experts) to set policy and oversee the network.

important cyber security agency: CDCiber, the Brazilian Army's Cyber Defence Center (Muggah & Thompson, 2017, p. 3). CDCiber received US$ 60 million in funding in its first year, and the Brazilian government planned to allocate US$ 420 million through 2035, giving it greater institutional capacity than other cyber-focused agencies in the Brazilian system (Canabarro & Borne, 2013, p. 6; Diniz, Muggah, *et al.,* 2014, p. 26). Some authors nevertheless argue that CDCiber's funding is insufficient, given the importance of its mission (Diniz, Muggah, *et al*., 2014, p. 27; Modena, 2012).

CDCiber is so important that it has, over time, developed its own cluster of associated agencies to provide command, support, training, and tactical functions. In 2016, a joint Cyber Command (ComDCiber) was established to govern CDCiber, with representatives from all Brazilian armed services including the Navy and the Air Force (Hurel & Lobato, 2018, p. 8). Within the hierarchy of military planning, ComDCiber and CDCiber operate at the strategic level. Underneath CDCiber, there is a Joint Cyber Defence Detachment (JCDD) which is responsible for cyber conflict at the operational level, as well as a Joint Detachment of Cyber Warfare (JDCW) that is responsible for cyber conflict at the tactical level (Da Silva, 2019, p. 10). The Brazilian military also has a coordinating group, the Cybersecurity and Defence Coordination Center (CCSDCiber), and a training facility, the National School of Cyber Defence (ENaDCiber).

Brazil also possesses several civilian agencies that deal with cyber security. At the cabinet level, the Brazilian government has an Institutional Security Bureau (the GSI), which is roughly analogous to the Ministry of Intelligence found in the political systems of many other countries. This cabinet department contains a Department of Information and Communication Security (the DSIC-GSI). The latter group is tasked with coordinating the various CSIRTs of the Brazilian government, including CTIR.Gov (Hurel & Lobato, 2018, p. 7). The Brazilian National Information Security Policy (PNSI), enacted in 2018, centralised the oversight and coordination of information security under the GSI (Brazil, 2018). Building on this foundation, Brazil published a National Cybersecurity Strategy, or "E-Ciber", in 2020, which reiterates the GSI's coordination role while delegating responsibility for cyber defence to the military (GSI, 2020). The E-Ciber proposes several policy reforms, including a centralised system of cyber security governance at the national level, improved protection for critical infrastructure, increased cooperation with other governments and non-state actors, and the development of a new legal framework for cyber security (GSI, 2020). In addition, there is another important non-military actor in the Brazilian system: the Brazilian Intelligence Agency (ABIN). ABIN began monitoring Brazilian social networks in the aftermath of protests in 2013 and houses a Centre for Research and Development of Secure Communications (CEPESC) to handle cryptography and

ensure secure communications within the Brazilian government (Diniz, Glenny, & Muggah, 2014, p. 20).

A third actor, in addition to military and civilian intelligence agencies, is the Brazilian police (Muggah & Thompson, 2017, p. 4). The Brazilian Federal Police contains a dedicated Unit for Combating Cybercrime (the URCC),[66] which investigates online crimes such as financial fraud or the distribution of child sexual abuse imagery (Diniz, Glenny, *et al*., 2014, pp. 9, 22-23). The URCC is in turn tasked with coordinating the growing number of specialised cyber crime units within the police forces of the 26 states (Diniz, Glenny, *et al*., 2014, p. 23).

What are we to make of this large and complex cyber security system? On the one hand, the creation of a "sprawling cybersecurity and defence infrastructure" (Diniz, Muggah, *et al*., 2014, p. 3) indicates the high level of importance that the Brazilian state assigns to the issue. On the other hand, the size and complexity of the Brazilian system has arguably reduced its effectiveness (Hurel, 2020). At the cabinet level, responsibility for cyber security is spread out across three different ministries: Defence (responsible for CDCiber), Institutional Security (responsible for ABIN), and Justice (responsible for the URCC). Several policy analysts have argued that the Brazilian cyber security system is too complex to function effectively**:** Hurel and Lobato (2018) criticise the "absence of efficient mechanisms for collaboration", while Diniz, Muggah, *et al.* (2014, p. 29) complain about the "lack of coordination between government institutions". Da Silva (2019, p. v), a colonel in the Brazilian army, argues that these problems could be addressed by creating a new "cybersecurity control body" to coordinate the defence of critical infrastructure; but this would probably make the current system even more unwieldy. Instead of creating new coordination bodies, Brazil would probably benefit from having fewer agencies with better funding and clearly demarcated areas of responsibility.

Several scholars have also voiced normative criticisms of the Brazilian cyber security system. For example, Canabarro and Borne (2013, p. 10) criticise Brazilian cyber strategy for simplistically defining "state and non-state actors… as major foes". Politically-motivated hacktivists[67] have been classified as "security threats", without a nuanced consideration of whether their motivations and methods are legitimate (Canabarro & Borne, 2013, p. 10). Lobato and Kenkel (2015, p. 31) critique

[66] In some sources, this is anglicised as the Cyber Crimes Repression Centre (SRCC). See Cordeiro (2017, p. 4), for example.

[67] "Hacktivists" are private individuals, not affiliated with any state, who use computer hacking to advance their social or political goals.

what they see as a pattern of "hypersecuritisation", in which the Brazilian government creates "catastrophic scenarios […] of cascading disasters" to justify the extension of military authority into the cyber domain. Diniz, Muggah, *et al.* (2014, p. 4) argue that the "militarisation" of cyber security has not been driven by Brazilian national interests, but instead by the narrow bureaucratic interests of the Brazilian army, which has struggled to find a role for itself in the country's current era of democratic governance. They argue that the most realistic cyber security challenge facing Brazil is online crime; and yet, instead of dealing with this genuine problem, Brazil's security establishment has allocated resources to counter the still-hypothetical problem of cyber warfare by other states (Diniz, Muggah, *et al.,* 2014, p. 23). A similar argument is advanced by Hurel and Lobato (2018, p. 2), who suggest that Brazil's excessive fear of cyber attacks against the state has caused it to ignore the more pressing problem of cyber crime against Brazilian citizens.

Setting these normative questions aside, we can also pose an empirical question: *why* did Brazil, a state which has historically faced minimal external security threats, choose to develop this elaborate, complex, and militarised set of cyber security organisations? Historically, the proliferation of Brazilian cyber security agencies was driven by two major developments, both of which increased the security pressures on the Brazilian state and forced it to re-evaluate its cyber security policies: the Brazilian policy of increasing its international prestige through the hosting of "mega-events", and US surveillance activities revealed by Edward Snowden. [68]

Brazil's policy of hosting mega-events was undertaken during the first administration of Lula da Silva and his successor Dilma Rousseff. This policy aimed to boost Brazil's international prestige, signal the country's status as an emerging power, and promote domestic economic development (Grix, Brannagan, & Houlihan, 2015, pp. 474-477; Grix, Brannagan, & Lee, 2019, p. 43). The most important of these mega-events were the 2014 FIFA World Cup and the 2016 Rio Olympic Games. However, Brazil also hosted several other significant events during the same period: the UN Conference on Sustainable Development in 2012; the visit of Pope Francis to Brazil in 2013; the Catholic Church's World Youth Day in 2013; the FIFA Confederations Cup in 2013; and the 2016 Paralympic Games (Diniz, Muggah, *et al*., 2014, p. 14). These events created new security challenges for the Brazilian state, stoking fears of terrorism, crime, football hooliganism, and violent social protest (Wong & Chadwick, 2017, pp. 7-10). In response, the government created a Special Secretary of Security for

[68] For more in-depth discussion of these historical developments and their impact on Brazilian cyber security strategy, see Hurel and Lobato (2018, p. 10), Diniz, Muggah, *et al*. (2014, p. 14), and Muggah and Thompson (2017, p. 4).

Major Events (Interpol, 2014), and deployed the Brazilian army to "pacify" the notoriously crime-ridden *favelas* that surround Rio de Janeiro (Rekow, 2016, pp. 6-7). These mega-events also provoked fears of cyber insecurity and cyber terrorism (Giulianotti & Klauser, 2012, p. 319).

When CDCiber became operational in 2011, its first major task was to ensure network security during the 2012 Conference on Sustainable Development (colloquially known as the Rio+20 conference) (Muggah & Thompson, 2017, p. 3). During the Rio+20 conference, a group of hacktivists claiming to represent "Anonymous Brazil" carried out a series of attacks against websites associated with the event and the Brazilian government. The hackers, who coordinated their actions using the Twitter hashtag "#OPHackinRio", boasted that they had "attacked dozens of websites" (Anonymous, 2012). In reality, these attacks were neither particularly sophisticated nor especially harmful. A total of 23 websites were either defaced or taken offline by DDoS attacks but were soon restored (Rohr, 2012). Nevertheless, the incident provided a justification for CDCiber's newfound role as a provider of cyber security for civilian mega-events (Diniz, Muggah, *et al.*, 2014, p. 14). That role was further strengthened during the 2014 FIFA World Cup and the Rio Olympic Games, which attracted similar attacks by politically-motivated hacktivists (N. B. Thompson & Muggah, 2016). During these mega-events, CDCiber increasingly took on the responsibility of coordinating the cyber security activities of the Brazilian military, Federal Police, and various CSIRTs (Hurel & Lobato, 2018, p. 11).

A second factor that drove the growth of Brazil's cyber security infrastructure was the information leaked by the American intelligence contractor Edward Snowden. In 2013, the Brazil-based journalist Glenn Greenwald published a front-page story in the newspaper *O Globo*, drawing on information he had received from Snowden, which revealed that the American NSA had conducted massive and indiscriminate surveillance of ordinary Brazilians (Greenwald, Kaz, & Casado, 2013). This was soon followed up by two further revelations that were even more explosive. First, it emerged that the NSA had spied on the personal communications of Brazilian President Dilma Rousseff (Bridi & Greenwald, 2013). More controversially still, the NSA had conducted what appeared to be commercially-motivated espionage against Petrobras – the crown jewel of the Brazilian public sector, and a key component of Brazil's economic development strategy (Reid, 2014, pp. 153, 259).

Public outrage over the Snowden leaks provided a justification for the Brazilian government to strengthen the country's cyber security agencies (Pedro, 2016, p. 303). In addition, the Brazilian government responded with several new policy initiatives. One such measure was its sponsorship of a new undersea cable, known as EllaLink. After its completion in 2021, this cable allowed direct

internet traffic between Brazil and Europe, bypassing servers and routing equipment in the United States. The Brazilian government also developed new regulations that would have required international technology companies (such as Google and Facebook) to store Brazilians' personal data on Brazilian servers; however, the local storage requirement was later dropped after it proved impractical (Boadle, 2014).

Brazil also responded to revelations through diplomatic pressure and by mobilising partnerships with other states. In 2013, President Dilma Rousseff took the unusual step of cancelling a state visit to Washington DC, which had been intended to signal the improved relations between Brazil and the United States under the administration of Rousseff and her counterpart Barack Obama (Erthal Abdenur & Frederico Pereira da Silva Gama, 2015, p. 464). One week later, Rousseff delivered the opening speech at the UN General Assembly, in which she elevated the surveillance issue to the top of the international agenda (Erthal Abdenur & Frederico Pereira da Silva Gama, 2015, p. 465). In her speech, she criticised the United States for its "invasion and capture of confidential information", which she described as a "grave violation of human rights" and a "disrespect to national sovereignty" (Rousseff, 2013, p. 2). Brazil and Germany then cosponsored a successful General Assembly resolution on internet privacy (Grigsby, 2014). Brazil was also able to mobilise support from its BRICS partners, such as South Africa (Mitrovic & Thakur, 2019, p. 253). Interestingly, these tactics appear to have been relatively successful. The Obama Administration did not give in to Rousseff's request for a public apology, but it sought other ways to placate Brazil and privately assured Rousseff that it would avoid excessive spying in the future (Bevins, 2015).

4.2.2 Refraining from Using Its Offensive Capabilities

In the aftermath of the Snowden revelations and the 2012-2016 mega-events, Brazil developed a significant set of technical cyber capabilities, with CDCiber and its associated constellation of military commands emerging as the country's flagship cyber security agency. Having invested significant resources in creating these capabilities, Brazil could have used them offensively to carry out technical cyber operations against other states. Instead, Brazil has used its cyber capabilities sparingly, for defensive and internal security purposes. Brazilian intelligence agencies have been criticised for spying on Brazilian citizens (Diniz, Muggah, *et al*., 2014, p. 15), but there is no evidence that Brazil has ever launched a major cyber operation against another state. On the contrary, the Brazilian use of technical cyber power as a tool of foreign policy has been remarkably restrained.

To demonstrate this, we can consider evidence from two datasets that track large-scale cyber operations: the CFR Cyber Operations Tracker (2022), and the CSIS Significant Cyber Incidents List (2023). In the CFR dataset, there are no incidents in which Brazil is coded as the aggressor. In the CSIS dataset (which includes major cyber crimes and state-sponsored cyber operations), there is one incident: an incident in which "Brazilian hackers carried out a cyberattack on the National Malware Centre website belonging to Indonesia's State Cyber and Password Agency" in October 2021 (CSIS, 2023, p. 18). However, this was probably carried out by non-state criminals. By contrast, the CSIS lists four incidents in which Brazil is coded as the defender: a ransomware attack in 2021, an attack on a pharmaceutical company in 2021, an attack on the domain name of a Brazilian bank in 2016, and a series of phishing attacks against tourists during the 2016 Olympic Games (CSIS, 2023, p. 20). The CFR dataset (which is entirely focused on suspected state operations) lists twelve incidents between 2013 and 2022 in which Brazil was targeted by foreign APTs. Among the attacking APTs were groups such as "the Dukes", "Careto", "Regin", "Machete", "Sowbug", "APT10", and "Operation GhostSecret". A diverse group of countries are suspected of sponsoring these APTs, including the United States, Russia, China, North Korea, and perhaps Spain – although definitive attribution of state-sponsored cyber operations, as always, remains difficult. In all these incidents, the attacker's motivation is coded as espionage, rather than sabotage or political subversion.

The Brazilian government does not appear to control any APTs of its own. In 2016, Kaspersky announced with some fanfare that it had discovered the first Portuguese-language APT, which it codenamed "Poseidon" (Kaspersky, 2016). Poseidon uses customised software and social engineering tactics, with the aim of stealing valuable commercial information from businesses (Gorobets, 2016). Although the group's language preferences indicate that it is almost certainly based in Brazil, it is probably not sponsored by the Brazilian government. In its research report, Kaspersky (2016) states unequivocally that it does "not believe [Poseidon] to be a state-sponsored attack but rather a commercial threat player" – an unusually confident statement from a security firm that is known for its reticence and caution on matters of attribution.

Of course, it is difficult to prove any negative proposition, and this is especially so in the murky world of cyber politics. It is possible that Brazil has secretly carried out offensive cyber operations against other states but has covered its tracks with such skill and finesse that no other states or private security researchers have been able to detect it. Such a scenario stretches the boundaries of plausibility, however. Even the most stealthy and sophisticated APTs, such as the Equation Group, have been unable to conduct operations without leaving behind some trace of their activities

(Kaspersky, 2015a, 2015b). It strains credulity to believe that Brazilian security agencies would have been able to conduct similar operations while concealing their actions completely.

The most plausible explanation for the observed absence of aggressive Brazilian technical cyber operations is that Brazil has not conducted any. This suggests that Brazil has instead adopted a defensive and restrained approach to technical cyber power. This is a surprising deviation from Buchanan's (2017a) theory of the cyber security dilemma, which predicts that all technically-capable states are likely to engage in "defensive" hacking even if they have no aggressive intentions. However, Brazil's policy of restraint is consistent with the hypothesis presented in this study, which argues that in the absence of external security pressures, states will generally adopt a restrained approach to technical cyber power. In the case of Brazil, a low-threat international environment has encouraged a rational policy response: a technical cyber power strategy that is low-risk, non-aggressive, and does not erode trust in the security of Brazil's domestic networks.

4.3 Brazil's Restrained Approach to Persuasive Cyber Power

Having considered the use of technical cyber power – or rather, the absence thereof – in Brazilian foreign policy, we can now turn to Brazil's use of persuasive cyber power. Brazil's overall approach to persuasive cyber power is, similarly, one of restraint. Brazil does not appear to have ever carried out a large-scale persuasive cyber operation against any other state. There is no evidence that it has engaged in disinformation campaigns, and even its overt public diplomacy campaigns have been relatively restrained. The closest that Brazil has come to interfering in the information markets of other states has been to encourage other countries to emulate its own, relatively non-interventionist model of internet governance.

Brazil's domestic system of internet regulation suggests that it places a high value on maintaining epistemic trust within its domestic information market. In terms of its domestic internet, Brazil has free speech policies that generally allow its citizens to exchange and debate ideas online without fear that this discourse will be suppressed or compromised by disinformation. Sometimes, this desire to maintain trust in its domestic information market pushes Brazil in strange and unproductive policy directions. Certain branches of the Brazilian government – especially the judiciary – have engaged in awkward attempts to restrict online services. Certain sub-national actors within Brazil have also used online disinformation campaigns to advance their interests in the context of Brazil's domestic politics; however, it is difficult to find evidence that these operations

were sanctioned by the Brazilian state. In general, Brazilian citizens are free to discuss ideas and participate in the online information market. Let us now consider both of these policies in turn.

4.3.1 Internet Governance and Soft Power

There is evidence that covert persuasive tools, such as bots, disinformation campaigns, and falsified social media accounts, have been used by domestic Brazilian actors to advance their partisan political narratives (Arnaudo, 2018, pp. 135-142). However, there is little evidence that the Brazilian state has ever used such in the context of its foreign policy strategy, either to advance geopolitical interests or to influence online political debates in other countries. As in the case with the absence of Brazilian cyber attacks and APTS, discussed in Section 4.2 of this chapter, there are different ways to interpret this. It is, in principle, possible that Brazil *has* used persuasive cyber power covertly and has avoided being attributed. However, a more plausible explanation for this absence of evidence is that Brazil has indeed refrained from using persuasive cyber power as a tool of foreign policy.

This is not to say that the Brazilian state has no interest in the internet as a communication medium. On the contrary, Brazil has taken a keen interest in the issue of internet governance and has encouraged other states to emulate its domestic approach to online speech. In 2003 it issued the Brasilia Declaration, which was co-authored with India and South Africa and calls for "ending the digital divide" (DIRCO, 2003). This illustrates Brazil's general approach, which has been to collaborate with other states in the global South in support of more equitable access to the global Internet. At the NETmundial conference in 2014, Brazil presented its internet governance institutions (including its CGI.br, its Internet Governance Agency, and the *Marco Civil da Internet*, its domestic internet law) as models for other countries to follow (Almeida, 2014). One Brazilian diplomat, quoted by Segal (2016, pp. 217-218), explains Brazil's approach to the internet governance debate as follows: "We are always at the centre of these issues... Brazil is in a better position to offer new ideas. We have a very interesting domestic model to offer."

It is noteworthy that Brazil supported the multistakeholder approach to internet governance at NETmundial, in opposition to the state-controlled "multilateral" model that was advocated by Russia and China (Segal, 2016, pp. 218-221). The multistakeholder model is described by ICANN (2015) as a "process of governance or policy-making, which aims to bring together the primary stakeholders such as businesses, civil society, governments, research institutions and non-government organisations to cooperate and participate in the dialogue, decision making and implementation of solutions to common problems or goals". The multistakeholder governance model is currently used

to manage the domain name registry and the ongoing development of the Internet Protocol (IP), the communication protocol that routes traffic through the internet. The multistakeholder model is generally supported by the United States and its allies. On the contrary, authoritarian states such as Russia and China have historically argued in favour of the "multilateral" model of internet governance, in which governance functions would be transferred to the United Nations and voting privileges would be reserved for states. Brazil's support for multistakeholderism over state-centric multilateralism at NETmundial is an important data point that suggests Brazil has relatively little interest in trying to control the flow of ideas or political narratives on the global internet.

The absence of Brazilian persuasive cyber operations should not imply that Brazil has no interest in what foreign audiences think about it. In fact, Brazil has explicitly sought to advance its foreign policy goals through the use of "soft power": the attractive power of its culture, ideological values, and political narratives. Celso Amorim, who served as Minister of Foreign Relations for a period during the first Lula Administration, argues that soft power (which he defines as "the use of culture and civilisation, not threats") is Brazil's primary resource for achieving its foreign policy goals (Lustig, 2010). Rubens Ricupero, who served as Brazil's ambassador to the United States and its permanent representative to the United Nations, makes a similar argument: "Brazil… has almost no hard power, but has soft power, giving Brazil power of influence and example that the country would never attain through arms" (Ricupero, 2010).[69] Sales Bonfim, a colonel in the Brazilian Army, argues that "Brazil has soft power… this is what we have that has most value in the International System" (Chatin, 2016, p. 2). However, Brazil's soft pursuit has generally been explicit and benign and has not relied on disinformation campaigns designed to trick foreign audiences. Reid (2014, p. 260) argues Brazil's soft power is primarily grounded in its culture ("music, dance, football and way of life") and its combination of a "market economy, democracy and social progress", which serves as a "powerful example to the developing world". A 2015 Brookings Institution similarly observes that the "emphasis of [Brazil's] foreign policy on equity, inclusion and universal institutions appeals to many states, especially small and middle powers" (Trinkunas, 2015).

This approach to soft power has been relatively successful. Malamud and Alcañiz (2017, p. 7) argue that Brazil has carved out an influential role in the negotiations surrounding virtually every major issue of international significance. Brazil's success in global governance is "based primarily on diplomacy, on the wise use of its cultural charm, and on its growing role as a facilitator and cooperation supplier" (Malamud & Alcañiz, 2017, p. 7). When Dilma Rouseff responded to the threat

[69] English translation is quoted by Chatin (2016, p. 6)

of NSA surveillance, she did so drawing upon Brazil's soft power reserves, framing the United States as a threat to human rights and Brazil as a rights-respecting democracy (Erthal Abdenur & Frederico Pereira da Silva Gama, 2015, p. 466). It seems likely that Brazil lost some of its software power during the presidency of Jair Bolsonaro, when Brazil was subject to sustained international criticism for some of its actions, for example, its policy of clearing the Amazon rainforest and its perceived insouciance in the face of the Covid-19 pandemic (Ballerini, 2020). However, the underlying sources of Brazilian soft power predate Bolsonaro's presidency, and future Brazilian administrations will surely try to find ways to rebuild and increase this resource.

Overall, these examples illustrate that Brazil assigns a high level of importance to its soft power and its international reputation, which is transmitted to audiences in other countries in part through online channels. Brazil has also tried to influence global internet governance through participation in initiatives such as NETmundial. However, Brazil has not sought to promote a state-controlled model of internet governance, and it does not appear to have ever made use of disinformation campaigns or to have seeded subversive narratives into the social networks of other states.

4.3.2 Maintaining Trust in the Brazilian Information Market

This study suggests that a significant trade-off of employing persuasive cyber power is the risk that a state may unintentionally harm epistemic and institutional trust within its domestic information market. If this is the case, we would expect a state such as Brazil, which refrains from using persuasive cyber power, will place a relatively high degree of importance on the competing interest of maintaining a trustworthy domestic information market. For the most part, the case of Brazil is congruent with this expectation.

Although Brazil is classified as a middle-income country by the World Bank (2020), its level of internet use is high: 77% of its population are internet users, compared to a global average of 62.5% (We Are Social, 2022, p. 15). Brazil's population makes intensive use of social media.[70] In 2022, Brazilians spent an average of 3 hours and 41 minutes per day using social networks (We Are Social, 2022, p. 19). As a result, social media has become an important influence on Brazilian politics. In 2010, citizen journalists used social media to publicise Brazilian military operations in the *favelas* that might have otherwise gone unreported (Singer & Brooking, 2018, pp. 67-68). Brazil's 2013 mass

[70] For qualitative accounts of the societal changes caused by widespread social media adoption in Brazil, see Segal (2016, pp. 201-207), Nemer (2016), Singer and Brooking (2018, pp. 67-68), and Diniz, Muggah, *et al*. (2014, p. 5).

protests, which swept the country in response to rising transportation costs, were organised on Facebook and Twitter (Segal, 2016, p. 204). The unlikely rise of Jair Bolsonaro, who served as president of Brazil from 2019 until 2022, was driven in part by the popularity of right-wing Brazilian content creators on social media platforms, especially YouTube (Fisher & Taub, 2019). The subsequent electoral defeat of Bolsanaro and the return to power of the left-wing Workers Party were similarly driven by online activism and journalism – in particular, embarrassing inside details about Operation Car Wash, the sprawling corruption investigation that brought down the presidency of Dilma Rousseff (Greenwald, Demori, & Reed, 2019).

Social networks have been able to achieve this influence because Brazil generally chooses not to restrict the importation and exchange of ideas by its citizens. This policy can be quantified using the Freedom on the Net index – an index created by Freedom House (2022) in which states are ranked according to their level of online freedom. States are assigned a score from one to 100, with 100 being the most free, and one being the least free.[71] States with a score of 70 or higher are considered "free"; those with a score of 30-69 are considered "partly free"; and those with 29 or less are considered "not free". Between 2011 and 2022, Brazil's Freedom on the Net score fluctuated between 73 and 63, straddling the border between "free" and "partly free". The country's lowest score was recorded in 2020, largely due to harassment of journalists who were critical of the Bolsonaro government, but Brazil's score still places it within the top tercile of the index (Freedom House, 2022).

Brazil has constitutional provisions to protect free speech: "expression of thought is free" (Brazil, 2019, p. 15). Interestingly, the Brazilian constitution (which went into effect in 1988) is notable for its lack of protection of *anonymous* political speech – a provision that became much more significant after the subsequent development of the internet (Brazil, 2019, p. 15). However, with *Marco Civil da Internet,* Brazil has gone beyond the "thin" conception of online freedom required by its constitution. The legal and institutional framework that ensures this relatively high level of online freedom is the *Marco Civil*, a pioneering law that was intended to create a "bill of rights" for internet users (CGI.br, 2014). The *Marco Civil* was designed to ensure freedom of online expression, protection of personal data, and individual privacy (Medeiros & Bygrave, 2015, p. 124). It requires technology companies to ensure network neutrality and protect user data. In return, those

[71] Prior to the 2019 report the scores were flipped around, with one considered to be most-free and 100 the least-free. In this study, Freedom on the Net scores that were assigned from 2011 to 2018 are inverted in order to allow for consistent comparison across different time periods.

companies are granted “safe harbour” protection in cases where copyrighted or illegal information is transmitted over their networks by users (Medeiros & Bygrave, 2015).

The origins of the *Marco Civil* lay in a cyber crime bill that was first proposed in 2007 by a Brazilian member of congress, Eduardo Azeredo (Segal, 2016, p. 205). The Azeredo bill caused controversy due to its proposed harsh punishments for downloading copyrighted content – including up to four years of jail time (Segal, 2016, p. 205). In response, law professor Ronaldo Lemos (2007) wrote an article arguing that, rather than laying down criminal penalties for internet users, Brazil should instead create a civil regulatory framework that would specify the rights and duties of users, technology companies and the government. This argument caught on and civil society activists began to mobilise support for the proposal. In 2008, a petition calling for the withdrawal of the Azeredo bill was circulated and signed by 160,000 Brazilians (Ferreira, 2014, p. 30). As public opposition mounted, President Lula delivered a speech in which he echoed many of the criticisms of the Azeredo bill and endorsed the competing idea of a civil rights framework (L. I. L. da Silva, 2009). After Lula’s speech, the Ministry of Justice began to develop the *Marco Civil*. The Brazilian government used an innovative policymaking process: it created an online discussion platform on which civil society representatives and ordinary internet users were invited to comment on the legislation (Ferreira, 2014, pp. 32-33). In this way, key aspects of the *Marco Civil* were “crowdsourced” to technical experts and the public (O'Maley, 2016). The legislation was not immediately passed due to controversy over its “net neutrality” provisions, but the bill was revived in the aftermath of the Edward Snowden leaks, and in 2014 it was signed into law (Meyer, 2014).

The process that led to the creation of the *Marco Civil* was complex, but Brazil’s general preference for online free speech was an important factor. The backlash against the Azeredo bill created a rational fear among democratic political elites that voters would punish them if they supported this unpopular legislation. Democratic institutions allowed Ronaldo Lemos and other members of civil society to mobilise popular support for the alternative policy of creating the *Marco Civil*. Democratic institutions also created an incentive for the Brazilian state to open up the policy process to wider participation, if only to increase the likelihood that the resulting legislation would enjoy greater popular support. Finally, the outcry against US internet surveillance convinced Brazilian legislators to pass the law, despite the objections of telecommunications companies. In the years since the *Marco Civil* was passed, some observers have argued that the legislation has been only moderately successful in achieving its stated aims (Medeiros & Bygrave, 2015, pp. 129-130). Others, by contrast, view it as a successful example of multistakeholder governance that is worthy of emulation by other

states (van der Spuy, 2017, pp. 48-50). The key point is that the gains Brazil received from passing the *Marco Civil* could be undermined if Brazil were to make more aggressive use of persuasive cyber power as a tool of foreign policy.

The *Marco Civil da Internet* is an innovative law, but it has not been perfectly implemented. During the past decade, the Brazilian state has made several abortive attempts to regulate or manipulate online information flows. The Brazilian judiciary, in particular, has a tense relationship with technology platforms. In 2012, Brazilian police arrested a Google executive after the company refused to remove a controversial political video on YouTube (Sottek, 2012). In 2015 and 2016, Brazilian judges ordered three separate nationwide blockages of WhatsApp. All three cases were sealed, but the judges in each case implied the system of end-to-end encryption used in WhatsApp was the reason for the shutdown (Bhattacharya, 2016; Sreeharsha, 2016; Watts, 2015).[72]

Brazilian politicians have also made use of legislative and judicial processes to stifle online criticism. In 2009, Brazilian election law was amended to prohibit online media from promoting negative coverage of candidates for three months prior to an election, unless there is a specific "journalistic reason" for doing so (Article 19, 2009). Journalists or bloggers who disregard this law are subjected to fines or prison sentences (Freedom House, 2015). In 2016, a judge threatened Facebook with a nationwide block because one of its users created a fake profile that parodied a mayoral candidate (Carvalho, 2016). In 2016, a blogger who reported on corruption investigations into former president Lula da Silva was raided by the police (Fernandes, 2017). During the 2018 general election, politicians asked courts to remove critical posts on social media websites on at least 503 occasions (Ctrl+X, 2018). Glenn Greenwald, a journalist, was briefly charged with criminal hacking in 2020 after he published embarrassing details about Operation Carwash (Londoño & Casado, 2020).

Despite these periodic and often ham-fisted attempts to restrict online services, there do not seem to be any cases in which the Brazilian government has intentionally introduced misinformation into its domestic information market. Instead, Brazil has implemented free speech institutions such as the *Marco Civil*, which encourages Brazilian citizens to engage in online speech with confidence that they are not being manipulated or controlled by the government. This is what we would expect to

[72] End-to-end encryption, when implemented correctly, makes it difficult (or even impossible) for technology companies to comply with monitoring requests or intercept communications on behalf of governments. This is because the communications provider itself does not have access to the unencrypted information sent through its network.

see if Brazil has chosen to prioritise trust in its domestic information market and is consistent with other indicators of Brazil's restrained approach to persuasive cyber power in its foreign policy.

4.4 Brazil's Restrained Strategy

How should Brazil's cyber power strategy be understood in its entirety? Brazil consistently chooses to reduce its exposure to risk in the cyber domain, rather than increasing its freedom to act aggressively. Brazil does not appear to have carried out aggressive technical cyber operations, such as network intrusions or cyber attacks against its adversaries. Instead, the Brazilian strategy in the cyber domain is characterised by caution, conservatism, and self-restraint. This tendency to minimise risk was most evident during the country's response to the Snowden leaks. Unlike Iran (which responded to Stuxnet by launching the Shamoon malware attack), Brazil did not attempt to signal its offensive cyber capabilities or deter the United States. Instead of escalating tensions and provoking a possible cyber conflict, Brazil relied on less risky soft balancing tactics (Erthal Abdenur & Frederico Pereira da Silva Gama, 2015). It signalled its displeasure through diplomatic avenues, built coalitions with other affected states, and sought to establish new international norms that would isolate the United States.

This tendency to minimise risk can be seen in virtually every aspect of Brazil's cyber strategy. For example, there is no evidence that Brazil has ever attempted to subvert the institution of other states through online persuasion. Brazil has generally sought to promote internet freedom internationally; at NETmundial, for example, Brazil held up its multistakeholder institutions as a model for other countries to follow. These efforts are, in turn, underpinned by a self-confident belief that the free exchange of trustworthy information is likely to advance Brazil's national interests. This desire to increase trust is particularly evident in the policies that Brazil has undertaken to restore trust in the aftermath of the Snowden leaks, such as the data protection provisions of the *Marco Civil*. This policy is applied inconsistently and is sometimes undermined by Brazil's judicial and political elites. Nevertheless, Brazil's overall system of internet governance can be understood as an attempt to create a robust and reliable domestic information market.

In general, Brazil's cyber strategy in the cyber domain combines two principal elements: it has resisted using technical cyber operations against the networks of other states and it has also refrained from using persuasive cyber operations. Therefore, of the four ideal-types strategies discussed in Chapter Three of this study, Brazil's strategy most closely resembles the "restrained strategy".

Brazil's adherence to the restrained strategy is not perfect. Some Brazilian elites have taken actions that would seem to undermine trust in the country's cyber security and information markets. These include the failure of the Brazilian state to promote and protect strong end-to-end encryption, and the use of "fake news" (which is typically spread over WhatsApp) as a campaigning tool in domestic Brazilian politics. However, the general thrust of Brazilian cyber strategy has been to increase trust in networks rather than to improve its own technical or persuasive cyber capabilities.

		External Security Requirements	
		Low	High
Institutional Preferences	Positive	**"RESTRAINED STRATEGY"** Restrained use of technical cyber power Restrained use of persuasive cyber power **BRAZIL**	**"TECHNICAL-AGGRESSIVE STRATEGY"** Aggressive use of technical cyber power Restrained use of persuasive cyber power
	Negative	**"PERSUASIVE-AGGRESSIVE STRATEGY"** Restrained use of technical cyber power Aggressive use of persuasive cyber power	**"COMBINED-AGGRESSIVE STRATEGY"** Aggressive use of technical cyber power Aggressive use of persuasive cyber power

Figure 6: Brazil's location within the typology of cyber strategies.

4.5 Explanatory Variables

How should we explain Brazil's restrained strategy in the cyber domain? This is a topic that has not been extensively studied in the existing literature on international relations, with only a few research articles treating Brazilian cyber strategy as the dependent variable. Despite this, there are some explanations and theories in the current literature that we can analyse to gain insight into Brazil's

approach to cyber security. Furthermore, there are some potential explanations that can be dismissed pre-emptively, as they do not align with Brazil's observed behaviour.

First, we can safely reject one possible explanation: the possibility that Brazil's restraint in the cyber domain is explained by limited cyber capabilities. As this chapter documents, the Brazilian state possesses significant technological sophistication, as evidenced by its high internet usage and pioneering approach to internet governance. Furthermore, Brazil has made significant investments in cyber security capacity and training and has established a wide array of military, intelligence, police, and civilian agencies with expertise in this area (Devanny *et al.,* 2022, p. 9). It is also worth noting that countries with fewer resources than Brazil have managed to implement quite aggressive cyber strategies. In 2017, Ethiopia, one of the poorest countries in the world, successfully launched a cyber espionage operation against dissidents living abroad (Marczak, Alexander, McKune, Scott-Railton, & Deibert, 2017). It is reasonable to assume that Brazil could behave similarly aggressively if it wished. Therefore, Brazil's restrained strategy must be seen as a choice it has made, rather than a constraint it has been unable to overcome.

Second, we can probably dismiss the possibility that Brazilian cyber strategy has been strongly influenced by the personality of its leader or the ideology of its leadership. If this were the case, we would expect to see strategic shifts as the leadership passed from Lula to Rousseff and then to Bolsonaro. However, this research has not found evidence of such a shift; on the contrary, Brazil has displayed broad continuity in its cyber strategy across these different administrations. This suggests that there are deeper structural factors that drive its restrained approach in the cyber domain.

Domestic factors may play some role in shaping some aspects of Brazil's approach to persuasive cyber power; especially its domestic regulation of its information market and its approach to internet governance. Segal (2017, p. 204) suggests that Brazil's social culture might contribute to its high levels of social media use and the government's consequent reluctance to intervene too heavily in its information market. Segal (2017, pp. 205-207) also highlights the role of domestic institutions in leading to the passage of the *Marco Civil*. The popular backlash against the Azeredo bill created a rational fear among political elites that voters would punish them if they supported this unpopular legislation. In addition, Brazil's democratic institutions allowed Ronaldo Lemos and other members of civil society to mobilise popular support for the alternative policy of creating the *Marco Civil*. These democratic institutions also created an incentive for the Brazilian state to open up the policy process to wider participation, to increase the likelihood that the resulting legislation would enjoy

greater popular support. However, while these domestic-centred explanations offer useful insights, they do not fully explain why Brazil has resisted carrying out persuasive cyber operations or disinformation campaigns in other countries. As such, this approach should be supplemented with the understanding of institutional preferences and the offence-dominant nature of persuasive cyber power developed in this study.

Several scholars who have studied the emergence of Brazilian cyber power have explained this process as the result of Brazil's bureaucratic politics; in particular, the strength of the military as a domestic political actor. Brazil was directly governed by the military for a 21-year period from 1964 to 1985, and the military remains politically powerful, although it has struggled to find a role for itself in the democratic era. Many scholars who explain Brazilian cyber strategy in this way tend to share the normative and theoretical commitments of the Copenhagen School,[73] and are critical of Brazil's decision to "securitise" and "militarise" the cyber domain through the creation of military-controlled agencies such as CDCiber.

For example, Solar (2020, pp. 395-396) argues that Brazil is part of a wave of emerging democracies – both in Latin America and elsewhere – where the military has been able to position itself as the dominant force in cyber security through the creation of cyber command-and-control centres. Canabarro and Borne (2013, p. 10) argue that Brazilian cyber strategy has simplistically defined "state and non-state actors… as major foes". For example, politically motivated hacktivists have been classified as "security threats" without a nuanced consideration of whether their motivations and methods are legitimate. Lobato and Kenkel (2015, p. 31) critique what they see as a pattern of "hypersecuritisation", in which the Brazilian government creates "catastrophic scenarios […] of cascading disasters" to justify the extension of military authority into the cyber domain. Diniz, Muggah, *et al*. (2014, p. 4) argue that the militarisation of cyber security has not been driven by Brazilian national interests, but instead by the narrow bureaucratic interests of the Brazilian army. They argue that the most realistic cyber security challenge facing Brazil is online crime; and yet, instead of dealing with this genuine problem, Brazil's security establishment has allocated resources to counter the still-hypothetical problem of cyber warfare by other states (Diniz, Muggah, *et al*., 2014, p. 23). Hurel and Lobato (2018, p. 2) similarly argue that Brazil's excessive fear of cyber attacks against the state has caused it to ignore the more pressing problem of cybercrime against Brazilian citizens.

[73] See Chapter Two of this study for more discussion of the Copenhagen School of security studies, and the application of this theory to the cyber domain.

Although these explanations contain important insights into Brazil's bureaucratic politics and strategic culture, they do not necessarily help us understand the dependent variable of interest in this study. They help explain the growth of Brazilian cyber power, but they do not necessarily explain why Brazil has chosen to use its cyber power in ways that differ from those of the other states considered in this study.

If we consider Brazil from a comparative perspective, this puzzle is, in some ways, magnified. Both the United States and the Russian Federation also have strong, politically powerful militaries with a keen interest in developing offensive cyber capabilities. As Chapter Six notes, much of Russia's offensive cyber capability has been concentrated in its chief military intelligence agency, the GRU. Chapter Five points out that the key player in the United States is the NSA, which is a joint military and civilian intelligence agency located within the Department of Defence and led by a military officer. Thus, Solar (2020) is correct that the bureaucratic importance of the military in Brazilian cyber security agencies mirrors that in the global north. However, since similar bureaucratic factors exist in these other two states, this fact alone does not explain why these three states use cyber power in different ways.

To explain these differences, we need to step away from domestic variables such as bureaucratic politics or domestic political institutions. Instead, we must consider the role of structural and unit-level variables in shaping Brazil's cyber strategy. The following sections of this study argue that Brazil's use of cyber power can be explained more effectively by considering two unit-level variables: the relatively weak external security pressures facing the Brazilian state, and Brazil's broadly positive preferences with respect to international institutions.

4.5.1 Low External Security Pressures

Brazil's restrained approach to technical cyber power is consistent with the theory presented in this study, which argues that such a strategy is associated with low external security pressures. When the security requirements facing the Brazilian state increased, due to its policy of hosting mega-events that might have attracted terrorist attacks or other security problems, so too did its investment in technical security. However, the security pressures facing Brazil never reached the point where it became rational to launch offensive attacks. The low security pressures facing Brazil can be illustrated by its low level of military spending: 2005 and 2022, Brazil spent an average of 1.39% of its GDP on its military, compared to a global average of 1.93% (SIPRI, 2022). The underlying causes of

Brazil's low security requirements are its defensible geographic position and the absence of strong regional rivals.

With respect to its position in global politics, Brazil has been described as an "intermediate state" (De Lima & Hirst, 2006, p. 37), a "rising regional power" (Stephen, 2012, p. 292), and a "middle-ranking power" (Gardini, 2016, pp. 11-12). Brazil has several significant geopolitical advantages: a large population; vast territory; abundant natural resources; a diverse and vibrant national culture. At certain points in its history, Brazil's rate of economic growth has been spectacularly high; particularly during the late 1960s and the first decade of the 2000s. And yet, despite its impressive material resources, there are still lingering doubts about Brazil's claims to great power status. Brazil has never managed to sustain high economic growth rates for prolonged periods of time, and its military strength is mediocre. Brazil has also struggled to convince the smaller states in its own region to support the more ambitious elements of its foreign policy agenda, such as its plans for reforming the UN and the WTO (Malamud, 2011, pp. 9-10). For these reasons, Malamud (2011, p. 1) describes Brazil as "a leader without followers". A common refrain among sceptics is that Brazil is "the land of the future, and always will be" (Reid, 2014, p. 7). However, Brazil has the advantage of facing a regional political environment that does not pose obvious threats or security challenges.

Geographically, Brazil occupies a location that is isolated from other powerful states. Brazil's population, infrastructure, and economic output are concentrated in its southeastern region, in the dense urban centres of São Paulo, Rio de Janeiro, Belo Horizonte, Curitiba, and Porto Alegre. This urbanised coastal region is protected on its northern and western frontiers by the vast rainforests of the Amazon basin; terrain that is effectively impassable for any invading military force. On its eastern frontier, it is protected by the Atlantic Ocean and the "stopping power of water" (Mearsheimer, 2003, p. 113). Brazil's most important neighbours are the three states along its southern border: Uruguay, Paraguay, and Argentina. Together with Bolivia and Chile, these states make up the "Southern Cone" of the continent; this is the immediate region in which Brazil's geopolitical strategy is exercised. Brazil's geographic isolation has historically hampered its economic development, making it difficult to carry out domestic trade or export goods to overseas markets (Stratfor, 2012, pp. 5-13). However, it also means that Brazil is free from plausible military threats within its region.

During the nineteenth century, international relations in South America had a distinctly Hobbesian character, and Brazil fought a series of wars against the other states of the Southern Cone. Brazil

allied itself with Argentina and Uruguay in 1865, and the trio fought a brutal war against Paraguay which is estimated to have killed 60-69% of the Paraguayan population; the highest recorded casualty rate in the history of modern warfare (Whigham & Potthast, 1999, pp. 174, 185).[74] In 1903, Brazil expanded by capturing the province of Acre from Bolivia, thereby establishing the boundaries of the modern Brazilian state (Fifer, 1966, p. 364). In addition to these external conflicts, Brazil fought a long series of intra-state conflicts against provincial rebellions and revolutionary movements, many of which enjoyed foreign support (Reid, 2014, pp. 50-82). During the twentieth century, however, several systemic changes dramatically altered the politics of the region. Brazil consolidated its domestic monopoly on violence, settled its territorial disputes, and established a pattern of pacific relations with its neighbouring states. Brazil resolved most of its outstanding territorial disputes and settled its last major dispute (with Uruguay) in 1995 (Diniz, Muggah, *et al.*, 2014, p. 23; Simmons, 1999, p. 5). The result is that Brazil has not had to fight a war on its own territory since 1870.[75]

Traditionally, Brazil's main regional rival has been Argentina. During the 1970s and 1980s, both states were ruled by military regimes, and both harboured ambitions to build nuclear weapons (Matos, 2020, pp. 154-155). However, Argentina experienced a long and steady economic decline during the twentieth century, which ultimately rendered its claim to regional leadership untenable.[76] As a result, Argentina was forced to adopt a policy of *rapprochement* toward Brazil (Redick, Carasales, & Wrobel, 1995, p. 112). During the same period, Uruguay, Paraguay, and Bolivia became increasingly integrated with the Brazilian economy, transforming these states into *de facto* economic satellites of Brazil. In combination, these two developments have transformed the regional balance of power from one of latent bipolarity (in which Argentina might have plausibly hoped to form the central axis in a balancing coalition against Brazil) to one of latent unipolarity (in which Argentina has

[74] By way of comparison, the enormously destructive Nazi invasion of the Soviet Union during World War II resulted in the death of about 10% of the Soviet population (Whigham & Potthast, 1999, p. 174).

[75] There are a few partial exceptions to this general policy. In 1965, Brazil deployed troops to the Dominican Republic in a successful mission to support the government side of the Dominican Civil War (Ferguson, 1973, p. 536). In 1991, it briefly sent troops to Columbia in order to launch an attack against FARC (de Souza Pinheiro, 1995, p. 13). Brazil has participated in UN peacekeeping missions in the DRC, Mozambique, Angola, Guinea Bissau, East Timor, the Sinai Peninsula, the Gaza Strip, Lebanon, and Haiti (Alsina Jr, 2017, p. 7). Brazil also engaged in a non-violent military stand-off against France (the so-called Lobster War) from 1961 until 1963 (Azzam, 1964).

[76] Argentina was one of the wealthiest countries in the world in 1913, with a GDP per capita that exceeded many Western European states. However, after the economic shocks of World War I, Argentina experienced a century of economic stagnation and slow growth that effectively transformed it from being a rich country into an underdeveloped one. Argentina's economic history during the twentieth century is discussed in detail by Taylor (1992).

been forced to accept permanent second-tier status). As such, Brazil is now clearly the most powerful state in South America.

This position of regional power gives Brazil an important set of advantages. It discourages potential challengers, thus helping to create a region of the world in which "[i]nterstate war is an anomaly" (Balzacq, Dombrowski, & Reich, 2019, p. 13). Since Brazil does not face any revisionist challengers and is unlikely to fight a regional war, it has little need to follow a costly regional balancing strategy (Burges, 2008, pp. 67-68). Instead, it can focus its resources on its domestic economy. Unlike the United States, Brazil has little desire to project its power outside of its region or to frustrate the rise of potential hegemonic powers in other parts of the world. On the contrary, Brazil would prefer to live in a more multipolar world (Milani & Nery, 2019, p. 154). Therefore, in addition to avoiding the costs of regional balancing, Brazil is also able to avoid the costs of an offshore balancing strategy. The absence of direct regional threats and overseas military commitments means that Brazil is able to choose which military conflicts it wishes to enter, resulting in an unusually high success rate in war.[77] It is also notable that, despite the general increase in global terrorism that has occurred in the aftermath of the 9/11 attacks and the rise of the Islamic State (IS), Brazil has not suffered any deaths as a result of international terrorism.[78]

Brazil is not a satisfied power. Brazil would prefer to increase its international prestige, develop its economy, and gain a greater say in international governance, but it faces several external and internal problems that limit its range of viable strategic options. Externally, presence of US power in the Americas, established since the Monroe Doctrine and reinforced during the Cold War, continues to restrict Brazil's freedom of action (Weyland, 2016, p. 150). Internally, Brazil is constrained by problems such as its very high economic inequality, the problem of corruption among its political elites, its long history of regionalism and sectionalism, and extreme political polarisation between left-wing and right-wing factions in its domestic system. However, these challenges do not pose a fundamental threat to its security. Brazil's low external security requirements are ultimately grounded in its defensible geography, its relative power within its immediate region and its absence

[77] There is no Brazilian equivalent of the disastrous US and Soviet interventions in Vietnam and Afghanistan. On the contrary, every Brazilian military conflict since 1828 has ended with a broadly favourable outcome for Brazil.

[78] According to the Global Terrorism Database (START, 2019), Brazil suffered a total of 28 fatalities from terrorist attacks between 2006 and 2018. During this period, most terrorist attacks (25 out of 29) were carried out by unknown perpetrators; these were probably criminal groups. One attack was attributed to First Capital Command, a large criminal organisation. Only three incidents had clear political motivations. These included two attacks carried out by right-wing extremists, and one carried out by pro-Palestinian extremists. However, none of these three attacks inflicted any casualties.

of major extra-regional commitments, none of which is likely to change in the foreseeable future. As a result of this secure environment, Brazil has little need to resort to using technical cyber operations, with all the costs and trade-offs that this would entail.

4.5.2 Positive Institutional Preferences

Brazil has not only refrained from carrying out aggressive technical cyber operations – it has also avoided the aggressive use of persuasive cyber power. This strategic approach can be explained by the pro-institutional nature of Brazilian foreign policy. Brazil's institutional preferences can be broadly classified as "positive", in the sense that Brazil generally operates as an institution builder rather than working to undermine institutions with which it disagrees. This is a rational strategy for a mid-tier military power that relies on soft power, attraction, and institutional leadership to advance its political and economic interests. Brazil's preference for institution building is particularly evident in its relationships with other states in the global South, with which it has partnered to create institutions such as the Southern Common Market (MERCOSUR), the Union of South American Nations (UNASUR), and the BRICS group.

However, this should not imply that Brazil is uniformly supportive of the institutional *status quo*. In fact, Brazil holds several institutional preferences that can be fairly described as revisionist. A central Brazilian foreign policy preference, consistently held across democratic and non-democratic governments alike, is the desire for greater international prestige, and for a correspondingly greater say in institutional decision-making (Erthal Abdenur & Frederico Pereira da Silva Gama, 2015, p. 463; Stephen, 2012, pp. 308-309). In the aftermath of World War II, Brazil felt slighted by its inability to obtain a permanent seat on the UN Security Council. The goal of reforming the UN Security Council and securing a permanent seat for itself continues to be one of the most important long-term objectives of Brazilian foreign policy (Amorim, 2011; Milani & Nery, 2019, p. 154). There is a similar ambiguity in Brazil's relationship with the main hemispheric organisation, the Organisation of American States (OAS). While OAS membership does provide Brazil with a useful platform for North-South cooperation, the presence of the United States within the organisation tends to overshadow Brazil, making the OAS less beneficial to Brazilian interests than other regional institutions (Weiffen, Wehner, & Nolte, 2013, p. 382).

Another area in which Brazil wishes to adjust the institutional *status quo* is the area of global economic governance. Economic developmentalism has been another important constant in Brazilian foreign policy, regardless of regime type or domestic ideology (Burges, 2008, p. 77; De Lima

& Hirst, 2006, pp. 22-25). Brazil has traditionally been wary of international economic institutions such as the WTO as it harbours the suspicion that they cater primarily to the interests of wealthy countries. This scepticism has led Brazil to advocate for greater representation of developing states within these organisations and to attempt to position itself as the leader of a bloc of countries that wish to create a more equitable global economic order (Efstathopoulos, 2012; Hopewell, 2015).

However, even in the case of institutions that Brazil regards as inequitable, Brazil's approach remains positive rather than negative. For example, it has not attempted to reduce trust in the WTO; instead, it has sought greater leadership and influence within the WTO in an attempt to reform it (Efstathopoulos, 2012). In the case of the OAS, Brazil's strategy has been to develop and strengthen the role of more localised organisations in which it holds a dominant position. In particular, Brazil has relied on MERCOSUR to promote regional free trade and economic integration, and UNASUR to promote regional security cooperation. By developing and strengthening these regional institutions, Brazil has been able to pursue its interests more effectively and assert its leadership without the direct competition of the United States.

In the case of MERCOSUR, this institution serves the dual roles of establishing Brazilian economic hegemony in the Southern Cone and acting as a bulwark against the growth of US influence in the region. As Celso Lafer, who served as foreign minister to Fernando Henrique Cardoso, put it: "MERCOSUR is our future" (Vigevani & Fernandes de Oliveira, 2007, p. 61). Since MERCOSUR functions as a regional trading bloc, it gives Brazil a reasonable alternative to joining the proposed Free Trade Area of the Americas (FTAA), a US-driven initiative to extend the North American Free Trade Agreement (NAFTA) model to encompass Central and South America (Weyland, 2016, p. 156). If Brazil did not have MERCOSUR as an alternative free trade area, it would be in a weaker negotiating position relative to the United States and it would probably be forced to make significant concessions in order to join the US-dominated FTAA instead.

A similar dynamic exists in the case of the regional security organisation, UNASUR. This organisation was established in 2008 to foster regional integration and cooperation among South American nations, and Brazil played a key role in its creation and development. UNASUR provides Brazil with a mechanism to strengthen its ties with its South American neighbours and counterbalance the influence of the United States in the region (Weiffen *et al*., 2013). Brazil temporarily left UNASUR between 2019 and 2023, as a result of President Jair Bolsanaro's belief that UNASUR was a leftist organisation that accorded too much influence to Venezuela. However, even under Bolsanaro,

Brazil's instincts remained in place: instead of withdrawing from regional security organisations, Brazil tried to develop a rival institution, PROSUR (the Forum for the Progress and Development of South America), which would be dominated by itself rather than Venezuela.

From the early 2000s onwards, Brazil's institutional strategy has evolved and become more ambitious, extending beyond its traditional area of influence in South America. This shift was particularly noticeable during the first administration of President Lula, in which Brazil pursued a more assertive foreign policy that focused on building relationships with emerging powers across the globe. In 1999 Brazil joined the G20, a forum for international economic cooperation that includes both developed and developing states. In 2003, Brazil became a founding member of the India-Brazil-South Africa (IBSA) Dialogue Forum, a trilateral initiative that aimed to promote South-South cooperation. In 2009 it joined the BRICS Forum, an association of five major emerging economies comprising Brazil, Russia, India, China, and South Africa. These extra-regional partnerships have allowed Brazil to engage in a moderate form of "soft balancing" against the United States (Flemes, 2007, pp. 14-16).

In general, it is evident that Brazil has positive institutional preferences: it views international institutions as tools to be used rather than constraints from which to escape. Brazil has been an enthusiastic builder of regional institutions in South America, which it uses to extend its influence and maintain its position of regional leadership. More recently, Brazil has begun to build institutions to expand its influence beyond South America, seeking to align itself with other states of the global South. Even in the case of *status quo* institutions that Brazil perceives as unfair, such as the UN Security Council or the WTO, Brazil's policy has generally been to position itself as a leader of a pro-reform coalition within these institutions, rather than trying to subvert or undermine trust in these institutions.

This pro-institutional foreign policy is a rational strategy for Brazil to follow and is consistent with the expectations of realism (Weyland, 2016, pp. 145-147). Economic underdevelopment exerts a significant limitation on the freedom of action, so it is rational for it to try to change the economic *status quo*. While Brazil climbs the developmental ladder, it is also rational for it to portray itself as a cooperative state and forestall the emergence of a regional counter-balancing coalition. Official Brazilian statements on national strategy tend to emphasise economic goals such as regional trade, "South-South cooperation", and poverty reduction, rather than traditional realist goals such as military security (Ban, 2013, p. 13). However, Weyland (2016, p. 158) points out that a close

examination of Brazil's intra-American trade policy reveals an emphasis on relative gains rather than absolute gains, suggesting that the pursuit of self-interest is at the heart of Brazilian policy toward international institutions.

Since Brazil relies on regional institutions for economic development and to legitimise its regional leadership, reducing trust in these institutions would be contrary to its interests. This means that Brazil would have little to gain from making aggressive use of persuasive cyber power. As discussed in Chapter Three of this study, persuasive cyber power is essentially an offence-dominant technology: it is useful for undermining trust in institutions; however, with very few exceptions (such as its post-2019-2022 policy towards UNASUR), this is not the goal of Brazilian foreign policy. On the contrary, persuasive cyber power would be ineffective to realise Brazil's foreign policy interests in supporting the institutions that it wishes to promote. Since persuasive cyber operations would offer Brazil a low payoff, and would likely incur trade-offs and costs in the form of reduced trust in Brazil's domestic information market, it is rational for Brazil to refrain from carrying out such operations. Thus, Brazil's reluctance to use persuasive cyber power can be understood as a rational response to the strategic circumstances in which it finds itself.

4.6 Conclusion

This chapter argues that Brazil's cyber strategy can be explained by two primary factors: its external security requirements and its institutional preferences. Brazil has been fortunate enough to find itself in a secure regional environment characterised by defensible geography, an absence of strong regional rivals, and a lack of major overseas commitments. Furthermore, Brazil's institutional preferences are largely positive. It views international institutions as valuable tools to advance its national interests and regional leadership. As such, it has tended to focus on creating, strengthening, or reforming institutions rather than undermining those it perceives as constraining. These factors appear to have led Brazil to adopt a restrained approach to cyber power.

Brazil has invested in developing technical cyber capabilities but has refrained from using them offensively. There is no evidence that it has engaged in destructive cyber attacks or carried out intrusive espionage. In the absence of pressing security threats, Brazil seems to have concluded that there is no reason to carry out such operations and has rationally refrained from doing so.

Brazil has adopted a similarly restrained approach to persuasive cyber power. It has shown interest in internet governance and a general desire to increase its reservoirs of soft power. However, Brazil

has not participated in online propaganda campaigns or attempted to seed trust-eroding narratives in other states' information markets. While Brazil holds certain revisionist institutional preferences, such as its desire for a permanent seat on the UN Security Council, it has been more interested in creating new institutions than in undermining old ones. Without hostile institutions to serve as targets for a persuasive cyber campaign, Brazil has had little reason to conduct such a campaign.

This restrained approach stands in contrast to the more aggressive cyber strategies outlined in the two subsequent chapters of this dissertation. In the following chapter, Brazil's restrained cyber strategy will be contrasted with the much more aggressive cyber strategy adopted by another democracy, the United States of America.

Chapter 5
The United States

5.1 Introduction

This chapter considers the cyber strategy of the United States of America. The United States has emerged as an extremely capable actor in the cyber domain, characterised by its sophisticated technical capabilities and creative, aggressive strategies. With the elite hackers at agencies like the National Security Agency taking the lead, the United States has carried out audacious cyber attacks against its enemies and constructed electronic espionage systems with frightening reach and scale.

However, despite its vast resources, it faces inherent trade-offs and dilemmas in exercising cyber power. Indeed, we might say that there is something tragic about American cyber strategy. The United States' cyber strategy is, in important respects, sub-optimal and self-contradictory. In choosing to adopt it, the United States has inadvertently undermined its domestic cyber security, exposed its most successful firms to commercial risks, and encouraged other states to view it with suspicion and balance against it. Exploits developed by American intelligence agencies have been used to launch cyber attacks on American cities and US allies, including the United Kingdom and Ukraine. Moreover, the growing threat posed by America's cyber power has inspired its adversaries to devise unconventional means of counterbalancing it.

The United States' approach to persuasive power has, in many respects, been more restrained. In general, the United States seems to refrain from carrying out large-scale disinformation campaigns. Instead, the United States has pursued an "internet freedom agenda", in which it has tried to convince other countries to adopt its domestic model of lightly regulated online speech while also pursuing public diplomacy campaigns that are relatively limited in impact. But here we see, too, various paradoxes and dilemmas of the US cyber strategy. The aggressiveness of US technical cyber operations has ironically threatened the trust on which its persuasive cyber strategy depends. In some cases, the United States has tried to export encryption technologies to help circumvent censorship overseas, even as its own intelligence agencies were working to subvert and weaken these technologies.

American policymakers are aware of the strategy's inherent trade-offs, and many have expressed their doubts and concerns. However, few have attempted to fundamentally change it. The United States, in a sense, is trapped by a combination of external security requirements and institutional

preferences that its policymakers cannot fully control. As a global power and regional hegemon, the United States faces complex external security challenges that are global in scope and have strained the country's military and economic resources. The United States must also manage an extensive network of alliances and institutions, giving it a set of positive institutional preferences that are rooted in its position as the dominant *status quo* power in the international system. This combination of factors has led to the adoption of its distinctive and somewhat self-contradictory cyber strategy, in which the United States tries to maintain trust in its preferred institutions while also using technical cyber operations against its enemies.

5.2 The United States' Aggressive Use of Technical Cyber Power

The United States is the most capable state actor in the world in terms of technical cyber power (Valeriano *et al.*, 2018, p. 200). It possesses an extraordinarily sophisticated and well-funded SIGINT agency: the NSA, which employs many of the most talented computer hackers in the world.[79] The NSA's offensive unit, which was once known as the Tailored Access Operations (TAO),[80] is responsible for carrying out many of the most daring and ruthless cyber operations ever recorded (F. Kaplan, 2017, p. 134). The "Equation Group", an APT that is widely believed to be controlled by the TAO, has developed malware with the almost supernatural-sounding ability to infect a computer and remain resident after the machine has been completely wiped (Kaspersky, 2015b). The United States also has a military Cyber Command, which is technically under the control of the Pentagon but is co-located with the NSA at its headquarters in Fort Meade, with a single military officer commanding both agencies (Schoka, 2019). In addition, the United States possesses a host of other security agencies, both military and civilian, with expertise in cyber conflict (Rosenbach & Peritz, 2009, pp. 2-4). This security infrastructure requires a considerable ongoing investment: one estimate argues that total US government spending on cyber power in 2016, across all government agencies, was between $26 and $30 billion – roughly equal to the entire defence budget of Germany during the same period (Klimburg, 2017, p. 136).

However, the most distinctive feature of the United States as an actor in the cyber domain is not its level of capability, but rather its willingness to use this capability aggressively in pursuit of its foreign

[79] One computer security expert described the exploiters used by the NSA as "works of art", featuring "robust, reliable, anti-forensics, network IDS evasion techniques, static binaries for run-time... Beautiful" (Hickey, 2017).

[80] A 2017 report in the *Washington Post* reported that the TAO had been renamed Computer Network Operations, or CNO (Nakashima, 2017b). To avoid confusion this study will continue to refer to it as the TAO unit, since this is how it is described in most of the research literature.

policy goals. In this regard, the strategy of the United States differs markedly from that of Brazil, which is discussed in the previous chapter of this study. Although Brazil is significantly less capable than the United States in an absolute sense, it could almost certainly choose to carry out technical cyber operations if it wished to. However, Brazil faces a relatively non-threatening international environment, and it has responded to this environment rationally by opting for a strategy of self-restraint in the technical cyber domain. By contrast, the United States faces significant security pressures from the international system and has responded to these pressures by maximising its capabilities and aggressively using its technical cyber capability. This strategy is evident from the CFR Cyber Operations Tracker (2022), in which the United States is coded as the aggressor in 21 major cyber operations between 2007 and 2022.[81]

In the following sections of this chapter, US technical cyber operations are grouped into three categories, depending on the type of actor they are directed against. Firstly, the United States has engaged in cyber operations against non-state actors such as Al Qaeda and the Islamic State. Secondly, it has carried out cyber operations against so-called "rogue states". These are middle-ranking powers that the United States regards as violators of strategically-important norms – in particular, the norm against developing weapons of mass destruction. Thirdly, the United States has carried out cyber operations against other major powers, such as Russia and China. The following sections will consider each of these categories of operations in turn.

5.2.1 Waging the War on Terror

We begin by considering the use of cyber power by the United States against militarised non-state actors. The United States has engaged in nearly continuous military conflict against such groups since 2001, as part of a complex and multifaceted conflict that is officially known as the Global War on Terrorism, or more simply, the war on terror. These non-state actors are much weaker than states, both in terms of their conventional strength and their cyber capability (Weimann, 2005, p. 143).[82] Nevertheless, terrorist groups are disruptive and unpredictable, and the conflict against them was an overriding goal of US foreign policy under the Bush II Administration and, to a somewhat lesser extent, the subsequent administration of Barack Obama (J. M. Lindsay, 2011, pp. 766, 775).

[81] This largely corresponds with the data contained in the CSIS Significant Cyber Incidents List (2023).
[82] From a realist perspective, it has been argued the war on terror might be seen as a distraction from the more important foreign policy goal of balancing against rival states (Walt, 2012).

One early example of a cyber operation against a non-state adversary was the Real Time Regional Gateway (RT-RG) programme. Introduced in 2007, at the height of the Iraq War, this was one of the first documented cases in which the US used technical cyber power in an offensive capacity. At the time, the United States was under heavy pressure from fighting insurgents, and many contemporary observers had concluded that its military position in Iraq was on the verge of collapse (Negus, 2006; Rosen, 2005). In a latch-ditch attempt to salvage the position, the US introduced the RT-RG programme as part of a broader "surge" to counter the insurgency (F. Kaplan, 2017, pp. 158-160). The RT-RG allowed for intelligence analysis on an unprecedented scale: when it was first rolled out in Baghdad, it collected 100 million internet metadata records every day from that city alone (Moltke, 2019). According to a US official, the underlying philosophy was that instead of looking for "a single needle in the haystack", the NSA would instead attempt to "collect the whole haystack": every phone call, text message, and email sent in Iraq (Nakashima & Warrick, 2013). By collecting and permanently storing all Iraqi communications, the NSA would always have the option to re-analyse old data as new intelligence leads emerged.

At the operational level, the results were successful: the RT-RG drastically sped up the process of intelligence analysis and gave US forces a powerful new tool against the insurgency (SIDtoday, 2009, p. 4). At the strategic level, the surge (of which RT-RG was one component) contributed to a notable reduction in violence after 2007 (Stephen Biddle, Friedman, & Shapiro, 2012, p. 36). However, the United States was never able to achieve its pre-war goal of transforming Iraq into a stable pro-Western democracy that would be able to serve as a regional ally.

In parallel with the RT-RG, the United States developed an even more ambitious programme called "Turbulence",[83] which sought to apply the philosophy of "collecting the whole haystack" at the global level. This complex surveillance system was initially comprised of nine smaller programmes, to ensure technical redundancy and managerial efficiency (Gorman, 2007). It was able to collect "upstream" data from internet backbone cables, "downstream" data from online services, and "end-point" data from individual computers (Klimburg, 2017, p. 173). The upstream collection system, which was codenamed "Turmoil" at the time of the Edward Snowden leaks, was able to intercept packets sent through cables, satellites, and microwave transmissions (Sesek, 2014). These upstream efforts were supplemented by NSA efforts to tap directly into undersea cables, including the cables

[83] It should be noted that these internal codenames change frequently and have almost certainly been changed since the Snowden documents were leaked. As Klimburg (2017, p. 173) notes, the names of specific programmes are less important than the technical capabilities they represent.

that connect to Google and Yahoo data centres (Gellman & Soltani, 2013). Upstream collection was also supplemented by the cable-tapping efforts of allied intelligence agencies, including the British Government Communications Headquarters (GCHQ) (MacAskill, Borger, Hopkins, Davies, & Ball, 2013).

Meanwhile, downstream collection was facilitated through programmes such as "Prism", which gave the NSA a legal method for obtaining user data directly from large technology companies such as Microsoft, Yahoo, Google, and Facebook (T. B. Lee, 2013a). Initially, media reports on Prism in the aftermath of the Snowden leaks implied that the NSA had free and unrestricted access to the servers of these technology companies (Gellman & Poitras, 2013). Later, it emerged that the surveillance programme had been legally authorised under Section 702 of the FISA Amendments Act. Furthermore, collection requests had to be authorised in a court proceeding (albeit a secret FISA court), rather than collected in bulk (Brennan Center for Justice, 2013, pp. 2-3). Nevertheless, the Prism programme demonstrated the uncomfortably close relationship between the US intelligence community and technology companies that developed in the aftermath of the 9/11 attacks, as well as the strategic advantages that the United States gains from being the home of so many large technology companies (F. Kaplan, 2017, p. 194).

The NSA also developed advanced systems of end-point collection – that is to say, hacking into an adversary's computer and stealing their information directly. Historically, end-point collection NSA was usually conducted by the elite hackers of the TAO unit, using a variety of stealthy and sophisticated exploits such as "Quantum Insert" (Zetter, 2014b). Traditionally, the main disadvantage of end-point collection has been its time-intensive nature, but the NSA managed to speed up this method of intelligence collection through automation. At the time of the Snowden leaks, the NSA had created an automated hacking engine with the codename "Turbine", which was capable of targeting computers, exploiting them, and implanting malware without the need for a human operator (Gallagher, 2014). If we combine these capabilities with those of other sub-systems such as Turmoil, the overall picture of Turbulence that emerges is a system of surveillance that operates on an industrial scale: a system that sifts through vast quantities of internet traffic, identifies suspicious computers, and then automatically hacks into them to enable further intelligence collection (Sesek, 2014).

Why did the United States choose to construct this vast surveillance system? Although intelligence collected through Turbulence intercepts could be directed towards many foreign policy interests, the

primary motive for creating the system was the fear of terrorism. In the aftermath of the 9/11 attacks, it was widely assumed that non-state actors such as terrorists could not be deterred through the threat of conventional or even nuclear retaliation (Kean & Hamilton, 2011, p. 375). Thus, the United States adopted a raft of policies to forestall terrorist attacks before they could occur, including dramatically increased surveillance (Maras, 2010, pp. 21-22; McAdams, 2005, pp. 479-480). The Turbulence programme, in particular, was enabled by two key pieces of legislation, the FISA Amendments Act of 2008, and the Protect America Act of 2007 – both of which were explicitly designed as responses to the threat posed by groups such as Al Qaeda (Bush, 2008; T. B. Lee, 2013b).[84]

Some observers argue that this rhetoric is cynical and that the real motivation for the surveillance programme is to expand the power of the American government over its citizens (Greenwald, 2014, pp. 202-207; Snowden, 2019, pp. 204-205). However, a presidential commission appointed in the aftermath of the Snowden leaks – which included civil libertarians and prominent critics of the intelligence community – found that the NSA was indeed motivated by its counter-terrorism mission (Clarke, Morell, Stone, Sunstein, & Swire, 2014, pp. 141-145). Furthermore, these operations do appear to have paid some dividends: a *Washington Post* report implied that the TAO unit was involved in the effort to track down Osama Bin Laden (Whitlock & Gellman, 2013), and *The Intercept* has reported that the United States used metadata obtained by the NSA's surveillance programme to provide targeting information for lethal drone strikes (Scahill & Greenwald, 2014). This does not necessarily mean that the NSA surveillance system is sensible or ethical – only that it is unlikely that this programme would have been created in the absence of a terrorist threat.

As the threat from Al Qaeda receded, the United States began to use its technical cyber capability against another non-state actor, the Islamic State. Since this cyber campaign occurred after the Snowden leaks, the information about it in the public domain is somewhat vague. In 2016, US defence secretary Ash Carter revealed that US Cyber Command was attempting to degrade the Islamic State's IT infrastructure (R. Martin, 2016). The operation, codenamed Glowing Symphony, was designed to disrupt the communications, propaganda, recruitment, administration, and command-and-control networks of the Islamic State (Temple-Raston, 2019). Cyber Command

[84] The FISA Amendments Act and the Protect America Act were both controversial, but they ultimately passed because they were seen as necessary to satisfy the United States' external security requirements. During the debate over the Protect America Act, then-NSA director Mike McConnell lobbied successfully on behalf of the legislation by arguing that it was necessary for collecting "the information we need to prevent some horrendous act from taking place in the United States" (Kravets, 2008).

reportedly aimed to take over ten key accounts and servers that the Islamic State used to manage its IT infrastructure, using phishing as the initial method to gain entry (Temple-Raston, 2019). The operation was described, rather hyperbolically, as "dropping cyberbombs" on the Islamic State (Sanger, 2016b). However, according to a report by Sanger and Schmitt (2017), the results of the campaign were disappointing. Cyber Command succeeded in disabling the accounts, but the Islamic State quickly switched to a new IT infrastructure.

5.2.2 Opposing Nuclear Proliferation

While the United States was waging a cyber conflict against non-state groups such as Al Qaeda, it was also carrying out a second category of cyber operations against middle-ranking states that it considered to be rogue powers and nuclear weapons' proliferators. In this context, cyber operations have served as a low-cost alternative to conventional military operations.

This category includes the United States' cyber campaign against Iran, which is perhaps the most heavily studied campaign in the history of cyber conflict. The US-Iran cyber conflict is a particularly stark illustration of the causal relationship between external security pressures and the aggressive use of technical cyber power. Ever since 2002, when the Iranian nuclear enrichment facilities at Natanz and Arak were discovered, the United States has held a strong preference for preventing Iranian nuclear proliferation (Benjamin & Simon, 2019, p. 56; Dueck & Takeyh, 2007, pp. 191-192). Iran's nuclear ambitions also alarmed the United States' allies in the Middle East: between 2003 and 2012, Arab states such as Egypt and Saudi Arabia privately pushed for war, with the Saudi leader King Abdullah urging the United States to "cut off the head of the snake" (Zetter, 2014a, p. 191). The strongest calls for war came from Israel, which viewed the prospect of a nuclear-armed Iran as an existential threat and strongly urged the United States to launch an attack during the final year of George W. Bush's presidency in 2008 (Sobelman, 2018, p. 20). When Bush was reluctant to do so, Israel threatened to carry out an attack itself, but Bush refused to supply it with the necessary bunker-busting munitions and withheld permission to fly over US-controlled airspace in Iraq (Sanger, 2009).

The Bush II Administration was pro-Israel in its overall orientation, and it agreed that the Iranian nuclear programme posed a significant threat, but it was reluctant to become embroiled in a new Middle Eastern war at a period when it was already overstretched (Knowlton, 2007). At the time, the United States was supporting an overseas military deployment of 196,600 personnel in Iraq and 25,700 in Afghanistan, along with 288,627 personnel across 149 other countries as of December

2007 (C. Johnson, 2010, p. 121). In a 2008 poll, 90% of US military officers agreed that the military had "been stretched dangerously thin" by the Iraq War, and 80% agreed that the United States could not fight another major war (Reuters, 2008b). Bush feared that an Israeli strike would destabilise the region and perhaps ignite a new regional war that the United States would be ill-prepared to deal with (Bergman & Mazzetti, 2019).

As an alternative, the United States launched a covert campaign against Iran that made intensive use of cyber operations. This campaign, codenamed Olympic Games, demonstrated its technical cyber capability as well as its aggressive and risk-tolerant strategy. In the first phase of the operation, the TAO unit developed a "super malware" application known as Flame, which was used to scout out the Iranian network (Nakashima, Miller, & Tate, 2012). Flame made use of multiple exploits and combined them with a suite of surveillance capabilities, including the ability to record network traffic, take screenshots, log keyboard strokes, and record audio from microphones (Gostev, 2012). After mapping the Iranian network, the NSA then penetrated the network with a self-replicating worm that later became known as "Stuxnet" (Nakashima & Warrick, 2010). Although its file size was significantly smaller than Flame, Stuxnet also possessed an advanced set of capabilities: it used a stolen digital security certificate, was able to propagate itself using four zero-day exploits, could jump across air gaps using USB flash drives, and conceal itself from network operators to avoid detection (Langner, 2013, pp. 9, 11; Symantec, 2011). After inlecting the Siemens programmable logic controllers (PLCs) that controlled the Iranian centrifuges at Natanz, it began to subtly interfere with their operations, speeding them up and slowing them down to mimic natural equipment failures (Sanger, 2012a, p. 189). During the operation, the United States cooperated closely with Israel, which played a particularly important role in the Stuxnet testing phase. Israel went so far as to construct a replica of the Natanz facility, using Pakistani-made centrifuges, where the worm could be tested and debugged (Broad, Markoff, & Sanger, 2011).

Despite the significant resources invested in Olympic Games, the results of the campaign were mixed. The operation had to be aborted prematurely after Stuxnet spread beyond the confines of Natanz and was detected by Belarusian security researchers (Zetter, 2011). After Stuxnet was discovered, President Obama ordered the NSA to speed up the operation and destroy as many centrifuges as possible before it could be removed from the Iranian network. In the aftermath of the operation, a report by the Institute for Science and International Security suggested that Stuxnet destroyed approximately 1,000 centrifuges, representing approximately 20% of Iran's nuclear enrichment capability at the time (Albright, Brannan, & Walrond, 2010, p. 1). Ralph Langner, one of

the security researchers who discovered the malware, estimated that the operation set Iran's nuclear programme back two years (Y. Katz, 2010). However, subsequent scholarship has been more sceptical. Barzashka (2013) and J. R. Lindsay (2013) point out that Iran was able to replace its centrifuges quickly, and the long-term effects of Stuxnet appeared to be minimal. In 2014, Iran's total number of centrifuges had risen to 19,000, more than compensating for any losses caused by Stuxnet (Glaser, Zia, Mousavian, & von Hippel, 2014, p. 9).

However, there are legitimate reasons to consider Operation Olympic Games to be at least a partial success. The primary strategic goals of the operation were, first, to prevent the outbreak of a war between Israel and Iran, and secondly, to delay the nuclear programme long enough so that sanctions would force Iran to the negotiating table. In the end, both of these goals were achieved. Wendy Sherman (2018, p. 189), a US diplomat who negotiated with Iran, describes Stuxnet as one part of a broader package of policies that successfully forced Iran to the negotiating table. The cyber operation was only one part of a broader package of policies that included economic sanctions, coercive diplomacy, and covert actions. Israel carried out its own covert campaign against Iran, including a series of targeted assassinations of Iranian nuclear scientists (Bergman, 2018). In this broader context, Stuxnet signalled the capability and resolve of the United States, while undermining Iran's trust in its technical ability to develop a nuclear weaponry undetected and unchallenged. (Valeriano *et al.*, 2018, p. 199). The result of these negotiations was the Joint Comprehensive Plan of Action (JCPOA), which temporarily resolved the issue of Iranian nuclear proliferation before it was unilaterally abrogated by the Trump Administration (International Crisis Group, 2018, pp. 3-7).

Olympic Games was not the only US cyber operation against Iran. In the aftermath of the discovery and attribution of Stuxnet, security researchers discovered an entire family of malware applications that shared similar design principles to Stuxnet and Flame and appeared to originate from the same developers. Many of these were found to have infected computer networks belonging to Iran or its allies. This malware family included Duqu, a remote access trojan (RAT) designed for espionage (CrySyS, 2011); Gauss, a Stuxnet-like application that could steal funds from Lebanese banks (Goodin, 2013); Regin, a malware platform that could be used to attack a country's GSM cellular communication network (Kaspersky, 2014, p. 18); and ProjectSauron, an espionage-focused platform capable of jumping across air gaps (Goodin, 2016). The United States also created a plan for an exceptionally destructive cyber campaign, codenamed Nitro Zerus, that was conceived as a fallback option if the JCPOA negotiations failed (Buchanan, 2017a, p. 32). If activated, Nitro Zeus would have

entailed large-scale cyber attacks against Iran's military and civilian infrastructure, including its power plants, electrical grid, civilian communications, air defences, and military command-and-control networks (Ball, 2016). According to leaked reports from within the NSA, the initial stages of Nitro Zeus were actually put into practice, with many of these targets penetrated by the TAO as part of its mandate to "prepare the battlefield" (Sanger & Mazzetti, 2016). If the operation had gone ahead, it would have likely been the first true cyber war in human history. However, the successful conclusion of the JCPOA negotiations meant that there was no need to execute Nitro Zeus, and the attack was never carried out.

Between 2015 and 2018, while the JCPOA was in effect, there was a partial reduction in tensions between the United States and Iran. This resulted in a temporary lull in the cyberconflict between the two countries. However, after the Trump Administration withdrew from the JCPOA and reimposed sanctions on Iran, the conflict was renewed. Six oil tankers were attacked in the Persian Gulf in May and June 2019, and the United States blamed these attacks on Iran (Al Jazeera, 2019). Iran also shot down a US drone in June 2019 and was suspected of carrying out a drone attack against a Saudi oil field in September of that year (Gallagher, 2019). In response, the United States launched a new cyber campaign against Iran. This included a sabotage operation against an Iranian paramilitary group which the United States blamed for the tanker attacks (McLaughlin, Dorfman, & Naylor, 2019). According to a *New York Times* report, the operation temporarily disabled a database that the group had used to plan the tanker attacks, which temporarily reduced Iran's ability to carry out future attacks (Barnes, 2019).

At the same time, the United States was also conducting a cyber conflict with North Korea. Like Iran, North Korea is considered by the United States to be a violator of the strategically important norm of nuclear non-proliferation. However, the US-North Korea conflict differs from the US-Iran conflict in the important respect that North Korea is already a nuclear-armed state with the ability to attack US allies in the region, which reduces the United States' ability to credibly threaten it with a military strike. North Korea also differs from Iran in that it has pursued an economic strategy of "near-autarky" which reduces the effectiveness of US economic sanctions (Ho, 2017, pp. 117-124). Since the United States' ability to influence North Korea's behaviour through military or economic tools is limited, it has tried to find other means to exert influence, including the use of technical cyber operations.

However, US cyber operations against North Korea have been largely ineffective as a tool for coercion. After the 2014 Sony Pictures hack, which was attributed to North Korea, US President Barack Obama promised to respond "proportionally… in a place and time and manner that we choose" (PBS NewsHour, 2014). Hours later, North Korea experienced an internet shutdown that could have been the result of an American DDoS attack (Perlroth & Sanger, 2014). The shutdown only lasted nine hours (Walker, 2014), and presumably did little to influence future North Korean behaviour. In 2017, as part of the Trump Administration's "maximum pressure" strategy to extract North Korean concessions, US Cyber Command launched another DDoS attack – this time, against North Korea's Reconnaissance General Bureau (DeYoung *et al.*, 2017). However, North Korea was able to receive additional bandwidth from Russia, allowing it to easily counteract the effect of the US operation (Gallagher, 2017). More significantly, there were media reports that the United States had tried to sabotage North Korea's missile testing programme using a Stuxnet-style sabotage operation (Sanger & Broad, 2017). North Korea experienced several failed missile launches during this period; however, the failure rate was within the expected parameters, suggesting that if this cyber operation occurred, its effects were minimal (J. Lewis, 2017).

5.2.3 Engaging in Great Power Rivalry

A final category of US cyber operations encompasses operations conducted against other great powers, such as Russia and China. These states are distinctive in that they possess significant military capabilities – both conventional and nuclear – that would make any armed conflict against them extremely costly. The great powers in the international system thus have strong incentives to treat each other with caution, even in the cyber domain. This does not mean that they refrain from cyber conflict altogether. On the contrary, the global stability enforced by nuclear weapons may have the paradoxical effect of incentivising other forms of conflict behaviour that do not rise to the level of war, including cyber conflict.[85] However, cyber conflicts between the great powers tend to take the form of espionage operations, signalling exercises, deterrence-building mechanisms, and operations designed to improve the state's long-term strategic position. In general, these states do not engage in Stuxnet-style cyber attacks against each other – presumably because this type of aggressive sabotage has a high risk of spiralling into armed conflict.

[85] This is known as the stability-instability paradox; see Snyder (1965) and Watterson (2017). For specific applications of the paradox to cyber conflict, see J. R. Lindsay and Gartzke (2018) and Leach (2018).

The cyber conflict between the United States and Russia serves as a useful illustration of these dynamics. These two states have engaged in a long-running pattern of cyber espionage and counter-espionage that is, in many respects, an extension of Cold War-era statecraft. As was the case during the Cold War, these forms of subterfuge give the United States and Russia a useful method of engaging in rivalry without risking nuclear war. There are several notable incidents in which the United States has been the victim of alleged Russian espionage. It suffered major intrusions during the 1999 Moonlight Maze incident, the 2008 Agent.btz incident, and the 2020 SolarWinds hack (Healey, 2013, pp. 152-163, 205-211). However, the United States seems to have been even more successful in its attempts to penetrate Russian networks. The Equation Group (that is, the NSA's TAO) carried out a series of long-term espionage operations that were so effective that they went undiscovered for 14 years (Kaspersky, 2015a, p. 30). During the course of this cyber campaign, the Equation Group made use of an ultra-advanced malware platform called GrayFish, which could infect a targeted computer and then remain active even after a "military-grade disk wiping and reformatting" (Goodin, 2015). According to the intrusion report by Kaspersky (2015a, p. 20), Russia had the second highest number of Equation Group infections of any country in the world, after Iran. Russian government bureaucracies, military networks, research institutions, universities, and the energy, aerospace, telecommunications, and medical sectors were all successfully penetrated.

Great power competition between the United States and Russia intensified significantly in the aftermath of Russia's 2014 annexation of Crimea, its intervention in the 2016 US election, and its 2022 full-scale invasion of Ukraine. Since 2014, US cyber operations against Russia have become correspondingly more aggressive, going beyond passive espionage and attempting to directly frustrate Russia's pursuit of its foreign policy objectives. In 2018, the CIA successfully sought permission from the Trump administration to carry out aggressive cyber operations against Russia, Iran, and North Korea, without having to first obtain approval through the inter-agency decision-making process of the National Security Council (Dorfman, Zetter, McLaughlin, & Naylor, 2020).[86] In 2018, the Russian search engine Yandex was penetrated and implanted with the Regin malware platform (Bing, Stubbs, & Menn, 2019). Regin is used by the "Five Eyes" countries, i.e. the United States and its closest intelligence-sharing allies (Raiu & Kuznetsov, 2015). If the United States was indeed behind the 2018 infiltration, this would represent a notable example of US espionage against a Russian commercial entity (J. A. Lewis, 2016). During the United States' 2018 mid-term elections,

[86] This decision is significant because it allows for an increased tempo of cyber operations, and also because the CIA tends to emphasise covert operations, in contrast with the NSA's traditional emphasis on protecting its SIGINT sources (Chesney, 2020; F. Kaplan, 2017, p. 125).

US Cyber Command launched an operation to disrupt the actions of the Internet Research Agency (IRA), a Russian organisation based in Saint Petersburg that conducts persuasive cyber operations (Barnes, 2018; Nakashima, 2019). Most provocatively, the *New York Times* has reported that Cyber Command penetrated Russian critical infrastructure, including its power grid, and implanted logic bombs that could be activated in the event of a future conflict (Sanger & Perlroth, 2019). The story states that these actions are designed to create a deterrent effect and suggests that US policymakers viewed the operations as a form of "forward defence" rather than an act of aggression – a perspective that is, presumably, not shared by Russia. If the report is true, it would represent a major escalation of the cyber conflict between the two states.

Finally, there is evidence that the United States has carried out cyber operations against the People's Republic of China. In general, these actions have been less aggressive than its cyber operations against Russia. The Chinese national CSIRT has found that most hacking attempts against Chinese computers originate from IP addresses based in the United States (Haoran & Yusha, 2019), but the vast majority of these attacks probably originate from individual criminals rather than US government agencies. However, there have been some high-profile cases of US espionage against China. According to Kaspersky (2015a, p. 20), malware used by the Equation Group was discovered on computers used by Chinese diplomats and universities. The ProjectSauron malware platform, also used by US intelligence agencies, was discovered on a Chinese airline (A. L. Johnson, 2016). As the great power rivalry between the United States and China continues to intensify, resulting in greater external security pressures for both sides, it is almost inevitable that cyber conflict between these two states will escalate in tandem.

5.3 The United States' Restrained Approach to Persuasive Cyber Power

Perhaps the most intriguing feature of the United States' cyber strategy is the apparent disconnect between the way it uses the technical and persuasive forms of cyber power. As we have seen, the United States faces significant security pressures across the globe. It engages in conflict with non-state terrorist groups, weapons proliferators such as Iran and North Korea, and powerful rival states like Russia and China. In response to these pressures, the United States employs a variety of foreign policy tools, including coercive diplomacy, covert operations, conventional warfare, and the aggressive use of technical cyber operations. We might expect the United States to be equally aggressive in its use of persuasive cyber power, for example, through online propaganda and misinformation within the social networks of its many adversaries.

In fact, the United States' approach to persuasive cyber power has been relatively restrained. Although it has not entirely renounced online persuasion, the United States has mostly focused on promoting an "internet freedom agenda." It uses tools such as diplomacy, international agreements, and negotiations on internet governance to advocate for its domestic model of free and lightly-regulated online discourse. The United States has also invested heavily in online public diplomacy, beginning during George W. Bush's administration and redoubling these efforts under Barack Obama. These efforts represent the most direct use of persuasive cyber power by the United States. However, the United States appears to be reluctant to undermine trust in its domestic information market. Consequently, its public diplomacy campaigns have been overt rather than covert, which almost certainly reduced their effectiveness. Indeed, the United States' domestic system of internet regulation suggests that it places a high value on maintaining epistemic trust within its domestic information market. The United States has free speech policies that generally allow its citizens to exchange and debate ideas online without fear that this discourse will be suppressed or compromised by misinformation.

The following sections will consider the various elements of the United States' somewhat ambiguous approach to persuasive cyber power.

5.3.1 The Internet Freedom Agenda

The United States has long pursued the foreign policy objective of encouraging other countries to adopt open and unregulated information markets. This policy appears to stem from a conviction among US policymakers that free discussion and debate worldwide would ultimately benefit US interests. While this assumption does not always hold true, it has remained a consistent aspect of American policy under various administrations, with the partial exception of the Trump Administration. At times, this approach can become aggressive, such as when the U.S. exports censorship-circumvention technology to help individuals bypass internet controls imposed by their own governments.

Rhetorically, every US president since Bill Clinton has identified international "internet freedom" as a national interest (Goldsmith, 2018). However, it was George W. Bush who first elevated internet freedom from a general aspiration into a tangible goal of US foreign policy, and created permanent budgets and staffing structures to pursue this goal (MacKinnon, Wilson, & Woolery, 2016, p. 8). The Bush II Administration's preference for deregulated information markets fit naturally into its broader strategy of "democracy promotion", which in turn reflected its "Wilsonian" or "neoconservative"

approach to foreign policy (Jervis, 2003, pp. 366-368; T. Kahn, 2010, p. 17). In 2006, Secretary of State Condoleezza Rice announced that the US State Department would create a Global Internet Freedom Task Force (GIFT), a new group within the State Department that was given the task of promoting internet access across the world (State.gov, 2006a). The GIFT would be given the task of monitoring the level of internet freedom across the world, and would report attempts by governments to censor or control the internet so that US pressure could then be brought to bear on those countries (A. Ross, 2010, p. 12). In cases where diplomacy proved insufficient, the GIFT envisioned the creation of technical workarounds that could help dissidents in other countries circumvent internet censorship by their governments. To incentivise this, the GIFT created a $500,000 grant for software developers wishing to create "cutting-edge approaches to combat Internet censorship" (State.gov, 2006b).

After the Bush Administration was succeeded by the Obama Administration in 2009, US support for the internet freedom agenda was redoubled. In 2010, Secretary of State Hillary Clinton gave a speech at the Newseum in Washington DC, in which she observed that "asymmetrical access to information is one of the leading causes of interstate conflict" and argued that the free movement of information across national borders is likely to promote international peace and stability (Clinton, 2010). She summarised the United States' preference for single, globally-integrated online marketplace of information: "We stand for a single internet where all of humanity has equal access to knowledge and ideas" (Clinton, 2010). In a subsequent speech in 2011, Clinton expanded on these themes, defending the "marketplace of ideas" and focusing on the economic benefits of a free internet (Clinton, 2011). She also argued that cross-border flows of information should be reciprocal:

> As it stands, Americans can consider information presented by foreign governments. We do not block your attempts to communicate with the people in the United States. But citizens in societies that practice censorship lack exposure to outside views. In North Korea, for example, the government has tried to completely isolate its citizens from outside opinions. This lopsided access to information increases both the likelihood of conflict and the probability that small disagreements could escalate. So I hope that responsible governments with an interest in global stability will work with us to address such imbalances. (Clinton, 2010)

The Obama Administration undertook a series of actions to translate these ideas into policy. In 2010, the GIFT was renamed the "NetFreedom Task Force", and its stature within the State Department

was increased (CRS, 2016, pp. 3-4). In 2011, the United States announced its intention to form a Freedom Online Coalition (FOC): a bloc of states committed to the common goal of advancing internet freedom. The FOC originally consisted of 15 countries, but its membership has since expanded to 36 (FOC, 2023). The FOC provides an anchor of support for the US position in international debates over internet regulation – for example, most of the FOC states have voted with the US in international forums such as the 2012 World Conference on International Telecommunications, the 2014 NETmundial conference, and in the United Nations Human Rights Council (Maurer & Morgus, 2014, pp. 7-8; Zeldin, 2012).

In recent years, the United States has sought to introduce provisions on internet regulation into international trade agreements (Aaronson, 2017, pp. 237-238). The most notable example of this phenomenon was the proposed Trans-Pacific Partnership (TPP), which would have established common standards for online services alongside its more traditional provisions dealing with tariffs and subsidies. Although the United States ultimately did not ratify the TPP, Weber (2018, p. 12) argues that its goal during the negotiation process was to ensure a "liberal and deregulated internet, where US companies could export technology and information, and set US standards without any trade barriers or inhibitions from national regulators across the world".

The United States has also played an important role in debates over internet governance, due to its historical role in the development of the internet and its hosting of the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit corporation that is responsible for managing the global register of domain names and IP addresses. Internet governance became a contentious topic in international politics during the decade following 2010 when the narrow technical issues at stake became seen as proxy issues in the broader struggle to control the flow of information on the internet. In broad terms, the debate pitted the United States and its allies, which favoured the existing "multistakeholder" model of internet governance, against Russia, China, and their allies, which proposed switching to an alternative "multilateral" governance model (Trinkunas & Wallace, 2015, p. 3). The US position was that the internet domain name system should continue to be governed by ICANN, which includes representatives of business and civil society, as well as governments. By contrast, Russia and China argued that most of the functions to be transferred to the ITU, a more traditional international organisation located within the UN system, and whose membership consists exclusively of sovereign states (T. B. Lee, 2012).

Russia, China, and other states that favoured the ITU model argued that multistakeholderism was, in reality, a thinly-disguised form of US hegemony over cyberspace, and that it was necessary to "internationalise" the internet under the UN (Arsène, 2016, pp. 30, 33). Meanwhile, the US and its allies worried that multilateral governance would transform the internet into a state-controlled information network, effectively locking out civil society and other non-state actors (Kal, 2016, p. 500). They worried that, under this model of governance, authoritarian states would be in a position to incorporate mechanisms of censorship and control into the technical architecture of the internet itself, effectively balkanising the global internet into a series of disconnected national intranets and ending the free flow of information between countries (Hill, 2012). In the end, the US position won out, and ICANN retained its role in internet governance – thanks in part to Brazil's defection from the multilateral camp at the 2014 NETmundial conference (Segal, 2016, pp. 218-221). The United States did have to make an important concession to achieve this goal, however. To win international support for its position, it had to give up its control over the Internet Assigned Numbers Authority (IANA) and transfer these functions over to ICANN (Finley, 2016). With this relatively unimportant concession, the United States was able to achieve its broader foreign policy goal of protecting multistakeholder governance.

Going beyond its use of diplomacy and lobbying on the issue of internet governance, the United States has also used more aggressive methods to promote its stated goal of internet freedom. From 2003, the Chinese government rolled out its Golden Shield Project, which would eventually grow into the multi-layered system of internet censorship known as the "Great Firewall" (Qiu, 2003, p. 12). In response, American policymakers began to contemplate whether technical methods could be used to circumvent this type of online censorship. In 2004, three American computer scientists developed the Tor network, a system for routing internet traffic through sets of encrypted nodes that can be used to avoid government surveillance or censorship, with funding from the Defence Advanced Research Projects Agency (DARPA) and Office of Naval Research (ONR) (Dingledine, Mathewson, & Syverson, 2004, p. 15). According to a Freedom of Information Act request filed by Levine (2018, p. 238), almost all of the early funding for the Tor Project came from contracts with US government agencies such as DARPA, the Navy, and the State Department. With the benefit of these resources, the Tor Project was able to develop an anonymous web browser based on Mozilla Firefox, and eventually became one of premier tools for circumventing government control of the internet (Callanan, Dries-Ziekenheiner, Escudero-Pascual, & Guerra, 2010, pp. 41-42).

In 2009, in the aftermath of a disputed election result, the Iranian government was challenged by widespread protests known as the "Green Movement", which appeared to be using Twitter to coordinate its actions and spread its message (Sullivan, 2009).[87] In response, the State Department attempted to help the Green Movement, urging Twitter to delay a planned upgrade that would have temporarily cut off Iranians from the service (Pleming, 2009). American policymakers have long assumed that a more democratic Iran would hold foreign policy preferences that are more compatible with US interests (Weisman, 2005). That 2009 decision to ensure internet access for Iranian dissidents can therefore be seen as part of a long-term strategy to push Iranian preferences in a direction that suits US interests, and therefore an example of the United States making use of persuasive cyber power in its foreign policy. This was a very mild intervention, however; the United States did not do anything to actively help Iranian protestors, and only delayed a short, self-imposed service outage that had been scheduled by Twitter itself.

Nevertheless, the United States drew inspiration from the Green Movement and the events of the Arab Spring and increased support for censorship circumvention technologies. In 2015, the State Department unveiled its Leading Internet Freedom Technology (LIFT) initiative, which increased its funding to $33 million per year (Malinoswki, 2015). The State Department was joined in this task by the Broadcasting Board of Governors (BBG). This agency had been responsible for disseminating American viewpoints during the Cold War via broadcast networks such as the Voice of America, but it was reorganised in 2011 to focus on the issue of internet freedom. Initially, the BBG provided direct support for censorship-circumvention tools such as Psiphon, Tor, Ultrasurf, and Freegate (Marks, 2011). In 2012, the BBG (through its Radio Free Asia network) created the Open Technology Fund (OTF): a technology "incubator" that aimed to support the development of new anti-censorship and anti-surveillance technologies. In creating the OTF, the United States government sought to harness the venture capitalism of Silicon Valley in support of its geopolitical goals. Since its establishment, the OTF has supported several important technologies that are used to evade online censorship and surveillance by states, including the system of end-to-end encryption that is used in WhatsApp and Signal (Levine, 2018, p. 258).

The OTF was de-emphasised during the administration of President Donald Trump, prompting a writer for the Council on Foreign Relations to criticise the Administration's "lack of interest in

[87] The idea of the Iranian Green Movement as a "Twitter Revolution" was widely accepted at the time and informed the US policy response. However, subsequent scholarship has cast doubt on this interpretation of the 2009 protests. See Morozov (2009b) and Esfandiari (2010).

internet freedom and cyber diplomacy" (Fidler, 2017). Indeed, while the Trump Administration's official cyber strategy document called for "the free flow of data across borders" (United States of America, 2018, p. 15), the issue did not seem to excite the interest of the Administration's senior policymakers. In 2017, the newly appointed Secretary of State Rex Tillerson decided to close the Office of the Coordinator for Cyber Issues, which had previously dealt with the issues of internet freedom and cyber security (Chalfant, 2017). In 2018, Trump picked documentary filmmaker Michael Pack to lead the BBG (which had since been renamed the US Agency for Global Media, or USAGM); Pack then attempted to fire the entire leadership of the OTF and withheld $20 million in funding, forcing the fund to halt 49 of its 60 ongoing internet freedom projects (Cunningham, 2020).

It is not clear whether these changes represented a deliberate attempt by the Trump Administration to move away from the traditional US strategy of promoting the free movement of information. It seems likely that some of these changes were motivated by bureaucratic infighting, budgetary politics, and eccentric staffing choices, rather than any coherent attempt to alter America's persuasive cyber power strategy. Nevertheless, the Trump Administration's policies on internet freedom are consistent with a major theoretical claim of this study, which is that a state's approach to persuasive cyber power is directly influenced by its institutional preferences. Compared to previous Republican and Democratic presidential administrations, the Trump Administration was unusually suspicious and hostile towards international institutions. With these changing institutional preferences, it makes sense that the US policy on persuasive cyber power would shift as well. Since Trump was only able to complete one presidential term, he was unable to continue this change in strategy. However, if a future US administration resumed Trump's policies on international institutions, we should expect the US strategy on persuasive cyber power to shift along with it.

Even under presidential administrations that have chosen to emphasise the internet freedom agenda, the United States has been relatively unsuccessful in promoting this foreign policy goal. Although the United States managed to win a diplomatic victory at NETmundial and prevent any transfer of administrative control to the ITU, it has not been successful in its larger strategic goal of creating "a single internet where all of humanity has equal access to knowledge and ideas". On the contrary, states such as China that wish to censor and control their domestic information markets have continued to do so with great success. The United States has supported the development of censorship circumvention tools, but there are relatively few people who actually use these tools. Censorship circumvention software comes with significant downsides: it usually requires some technical skill; often has a negative impact on network performance; and may expose the user to

harmful repercussions from political authorities (Lam, 2019). A 2010 Harvard University report estimated that no more than 3% of the population of authoritarian states uses censorship-circumvention software (Roberts, Zuckerman, York, Faris, & Palfrey, 2010, p. 2012). Nevertheless, US policies on internet freedom can seem quite threatening from the perspective of authoritarian states.

For its part, the United States generally argues that its policies on internet freedom are essentially benign, since it does not carry out disinformation campaigns or other aggressive persuasive operations against its adversaries. Anne-Marie Slaughter (quoted in Lichtenstein, 2010), who served in the Obama Administration, summarises this view when she points out that "[w]e didn't put out propaganda to try to influence what was going on there… [w]e simply made it possible for people to continue communicating". However, for an authoritarian state such as China, which has observed events such as the Arab Spring and the Green Movement, and regards online censorship as an important tool for ensuring political stability, the internet freedom agenda can seem very threatening indeed.

5.3.2 Public Diplomacy

Through its diplomatic efforts to promote internet freedom, its lobbying over internet governance issues, and its aggressive sponsorship of censorship circumvention software, the United States has generally sought to promote the idea of a single, interconnected global information market. However, the United States has also actively participated in this market, by means of "public diplomacy" initiatives that are designed to communicate directly with global audiences through online platforms. These initiatives arguably represent the closest the United States has come to aggressively using cyber power. However, since these initiatives tend to be conducted overtly rather than covertly and typically aim to increase trust in the United States rather than reduce trust in the institutions of its adversaries, their effectiveness is relatively limited. Consequently, they likely have a minimal impact on the politics of other states.

Public diplomacy has long been a foreign policy tool of the United States (Zaharna, 2004, p. 220). American public diplomacy reached the height of its success during the Cold War when American radio stations such as Voice of America, Radio Free Europe, and Radio Liberty may have reached as many as one-third of Soviet citizens (Ash, 2010, p. 345). These radio channels were successful, in part, because the United States faced little competition, aside from the discredited media of the Soviet regime (Webb, 2017, p. 85). However, this is no longer the case in the digital era, where

online media have low barriers to entry and fierce competition. Moreover, the memetic transmission of ideas in social networks tends to favour emotionally charged content over truthful information. Consequently, the same qualities that made American public diplomacy successful during the Cold War – the size of its state-run broadcasting companies and its commitment to traditional norms of journalistic ethics – have arguably become disadvantages in the digital era.

Nevertheless, this has not stopped the United States from trying. In the aftermath of the 9/11 attacks, US policymakers quickly realised that the coming war on terror" would be, in part, a battle between competing narratives and ideas (Holbrooke, 2001). In 2008, George W. Bush appointed James Glassman as Under Secretary of State for Public Diplomacy and Public Affairs, and he pursued a new policy that he termed "Public Diplomacy 2.0". Under this policy, the United States would use digital technology to communicate directly with audiences in other states to advance "clearly defined national interest[s]" (Glassman, 2008). Initially, Public Diplomacy 2.0 was mostly focused on communication with the Muslim world, in an attempt to counteract the negative portrayals of the United States that are spread by extremist groups such as Al Qaeda. Compared to other US policymakers, Glassman was unusually quick to notice the offence-dominant nature of persuasive cyber power; he argued perceptively that "it's often more effective to destroy [US adversaries'] brand than build up ours" (Ackerman, 2009). In most respects, however, his approach was fairly conservative. For example, he directed members of the State Department's Digital Outreach Team to identify themselves as State Department representatives when engaging with social media, rather than spreading propaganda anonymously (Glassman, 2008). Furthermore, his approach remained grounded in traditional liberal assumptions about the truth-selecting nature of the market of ideas, leading him to implausibly argue that "[e]xtremists can't adapt to social networking" (Glassman, 2008).

In 2009, the Secretary of State Hillary Clinton appointed Alec Ross as her "Senior Advisor for Innovation". Ross and his subordinate Jared Cohen quickly became the most prominent advocates for Public Diplomacy 2.0 (or "twenty-first-century statecraft", to use their preferred term) in the Obama Administration (Cull, 2013, p. 20). Cohen and Ross' strategy was to use social media to amplify the effect of diplomatic outreach – for example, they organised online broadcasting of Barack Obama's 2009 Cairo speech, which attempted to repair America's frayed relationship with the Islamic world (Segal, 2016, p. 193). Ross and Cohen became mini-celebrities within US foreign policy circles, socialising with Silicon Valley tycoons and receiving a flattering profile in the *New York Times Magazine* (Lichtenstein, 2010). And yet, like Glassman, their approach was broadly

conventional. Ross and Cohen courted social media "influencers" and amassed followers on Twitter, but it is difficult to find any concrete evidence that these activities materially advanced US national interests. A congressional report from the period worried that their efforts "lack[ed] coordination and focus, and [might] fail to achieve strategic objectives" (GAO, 2009, p. 10). Morozov (2009a) dismisses Public Diplomacy 2.0 as "a new form of spam", observing that "whether one uploads press-releases from the State Department to one or twenty social networks is hardly going to have any influence on the situation".

Some US analysts, with greater insight into the conflict dynamics of persuasive cyber power, called for a new approach that would exploit the potential of memetic transmission of ideas. Prosser (2006, p. 10), a Major in the United States Marine Corps, argued that the Pentagon should embrace "military memetics", and proposed the creation of a "Meme Warfare Centre" within the military. Leetaru (2015), writing in *Foreign Policy* magazine, argued that the United States should create a "troll army" that would impersonate Islamic State members online, accuse real IS members of being US operatives, and disrupt the Islamic State's online recruitment efforts. In 2015, Jeff Giesea (2015, p. 73) – a member of the online "alt-right" movement, and a prominent online provocateur in his own right – published an article in *Strategic Communications*, an official NATO journal, which argued that the transatlantic alliance should embrace "memetic warfare" in its struggle against the Islamic State.

The United States has experimented with non-traditional and memetic approaches to public diplomacy. In 2011, the State Department established the Centre for Strategic Counterterrorism Communications (CSCC), which aimed to "de-radicalise" potential Al Qaeda and ISIS recruits. The first head of the CSCC, Ambassador Alberto Fernandez, fully embraced the offence-dominant logic of persuasive cyber power, stating: "[o]ur goal is not to make people love the US… [o]ur goal is to make al-Qaeda look bad" (Sanchez, 2014). Under Fernandez, the CSCC attempted to "troll" terrorist groups, picking online fights with their members and portraying them as hypocritical, sacrilegious, and stupid. When a pro-Jihadi Twitter account boasted about the "sincerity" of ISIS fighters, the CSCC tweeted back "You can best show your sincerity by not murdering women and children with suicide bombers" (Suebsaeng, 2014). In another tweet, the CSCC mocked the leader of ISIS, Abu Bakr al-Baghdadi, for wearing a Rolex watch (Cooper, 2016). In 2014, the agency published a controversial video called *Welcome to ISIS Land*; the video (which was viewed almost 900,000 times on YouTube) included footage of executions, severed heads, and crucified bodies (Miller & Higham, 2015).

This online campaign was widely criticised for legitimising the Islamic State and amplifying its propaganda (R. Katz, 2014). In 2015 Fernandez was removed from his position, and the CSCC shifted to a more traditional public diplomacy strategy (Miller & Higham, 2015). The CSCC's trolling campaign was short-lived and likely had minimal impact, but it serves as a useful demonstration of the trade-offs that constrain the US use of persuasive cyber power. While the criticisms of the campaign were valid, the CSCC demonstrated an awareness of the memetic nature of online information markets and sought to exploit these dynamics by creating content that was unconventional and irreverent, in stark contrast to the carefully hedged language that diplomats typically prefer (Segal, 2016, p. 2015). However, the fact that the United States chose to conduct this campaign overtly rather than covertly exposed it to criticism, and probably benefited the Islamic State rather than undermining it.

After the 2016 election of Donald Trump, the United States' use of digital public diplomacy underwent several important changes. Some of these changes were responses to shifts in the external environment. The CSCC was renamed the "Global Engagement Centre", moved away from its previous anti-radicalisation mission, and received a new mandate to counter social media disinformation campaigns by other states (Gabrielle, 2020). However, the overall policy of the Trump Administration was to de-emphasise and de-fund public diplomacy (Lynch & Gramer, 2020; Thrush & Davenport, 2017). For example, a 2020 report by the United States Senate (2020, p. 4) noted that the Under Secretary of State for Public Diplomacy and Public Affairs position had been vacant since March 2018, with no replacement candidate nominated. Hare (2020) argues that this neglect resulted from the intrinsic incompatibility between the methods of public diplomacy and the goals of Trump's "America First" foreign policy, which held little appeal for overseas audiences.

5.3.3 Maintaining Trust in the American Information Market

The United States, like Brazil, appears to assign a relatively high value to the goal of maintaining a domestic information market that is open and trustworthy. On the Freedom on the Net index, countries with a score of 70 or higher are considered "free", while those with a score of 30-69 are considered "partly free", and those with 29 or less are considered "not free" (Freedom House, 2022) The level of internet freedom in the United States decreased throughout the decade after 2010, falling from a high point of 88 in 2012 to a low point of 75 in 2021; as of 2022, it stands at 76 (Freedom House, 2022). There are several reasons why this ranking declined, including concerns about online surveillance in the aftermath of the 9/11 attacks, as well as concerns over more

traditional issues of censorship and government interference with online journalists (Aguilera, 2020; Fisher, 2014; Rafsky, 2011).

In recent years, as political attitudes in the United States have become more polarised, the question of how online information markets should be regulated has become increasingly fraught (Iyengar, Lelkes, Levendusky, Malhotra, & Westwood, 2019, pp. 131-134). Both Democrats and Republicans worry that social media companies offer an unfair advantage to their adversaries, creating a strong incentive for all political actors to attempt to tilt information markets in their favour (Bentley, 2016; Bogost & Madrigal, 2020). Prominent figures from both parties have threatened to revise Section 230 of the Communications Decency Act, a key legislative enabler that protects websites which publish user-generated content (Haberman & Conger, 2020; Molla & Stewart, 2019). Since 2020, the United States government has made several unprecedented attempts to ban the Chinese social networking platform TikTok, although it remains unclear whether these efforts will ultimately receive legislative and judicial approval (Bordelon, 2023; W. Ross, 2020). These policies may mark the start of a more restrictive approach to regulating online services in the United States, as the country grapples with the rising cyber power of China and its domestic consequences.

Despite these moves, it is important to stress that the domestic information markets of the United States are still lightly regulated compared to most other states. Compared to Brazil and Russia, the other two states examined in this study, the United States has the highest score on the Internet Freedom index by a large margin (Freedom House, 2022). This reflects the strong protection for free speech that is embedded in the First Amendment to the United States Constitution, which American courts have traditionally interpreted expansively. Online speech in the United States thus enjoys strong constitutional protections; even forms of expression that might be regarded as “hate speech” or “obscenity” in other legal jurisdictions (Sedler, 2006, p. 379). In general, there are only two types of online content that are excluded from these protections: material that is considered obscene (such as child abuse imagery) and material that is copyrighted. However, these exceptions have been interpreted narrowly. Attempts to expand these restrictions, such as the 2012 Stop Online Piracy Act and the restrictive provisions of the 1996 Communications Decency Act, have historically been struck through a combination of judicial review and legislative pressure (Mulligan & Bamberger, 2018, pp. 729-731).

5.4 The United States' Technical-Aggressive Strategy

How should we understand the cyber strategy of the United States in its entirety? In general, its cyber strategy has two distinctive features. First, the United States is exceptionally aggressive in its use of technical cyber power. It has executed massive surveillance operations targeting non-state actors, attempted to sabotage the weapons development programmes of states it regards as illegitimate nuclear proliferators and has engaged in complex strategic espionage operations against great power rivals.

		External Security Requirements	
		Low	High
Institutional Preferences	Positive	**"RESTRAINED STRATEGY"** Restrained use of technical cyber power Restrained use of persuasive cyber power	**"TECHNICAL-AGGRESSIVE STRATEGY"** Aggressive use of technical cyber power Restrained use of persuasive cyber power **U.S.A.**
	Negative	**"PERSUASIVE-AGGRESSIVE STRATEGY"** Restrained use of technical cyber power Aggressive use of persuasive cyber power	**"COMBINED-AGGRESSIVE STRATEGY"** Aggressive use of technical cyber power Aggressive use of persuasive cyber power

Figure 7: The United States' location within the typology of cyber strategies.

However, the United States has been much more restrained in its use of persuasive cyber power. It has promoted a global internet freedom agenda, which is admittedly quite threatening from the perspective of authoritarian states that prefer to maintain tight regulation over their domestic online discourse. It has also conducted public diplomacy campaigns through social media to enhance its image among overseas audiences. However, these efforts have been overt and there is little

evidence that they have had significant effects. Therefore, among the four ideal-type strategies identified in Chapter Three of this study, the approach used by the United States most closely resembles the "technical-aggressive" strategy.

This cyber strategy involves significant trade-offs and contradictions. By adopting this strategy, the United States has unintentionally exposed itself to several negative consequences: weakened domestic cyber security, increased commercial risks for its technology firms, and a heightened risk of other states forming balancing coalitions or engaging in retaliatory actions against it. The following sections examine these trade-offs and contradictions in greater depth.

5.4.1 Cyber Security Trade-Offs

The United States receives enormous benefits from the existence of an international communications network on which people and businesses can communicate privately and conduct commerce. However, by choosing a cyber strategy that involves aggressive computer hacking, surveillance, and electronic sabotage, the United States has implicitly chosen to subvert the security of this very same network. The general contour of this problem is familiar to US policymakers. Hillary Clinton (2010), speaking in her capacity as Secretary of State, observed that "those who disrupt the free flow of information in our society or any other pose a threat to our economy, our government, and our civil society." She added that "[c]ountries or individuals that engage in cyber attacks should face consequences and international condemnation", although she neglected to mention that at the time of her speech, the United States itself (in conjunction with its ally Israel) was carrying out the Olympic Games cyber operation against Iran.

Perhaps the clearest area where the trust trade-off arises in US policy is over the issue of encryption. Encryption enables secure online transactions and is thus a vital component of online commerce. Large technology companies – the source of much of the economic wealth and technical sophistication of the United States - are keenly aware of the importance of strong encryption for their business models and have encouraged their users to adopt it wherever possible. For example, Google encouraged the universal adoption of encrypted web traffic, while Apple has implemented full-device encryption on the iPhone since 2014 (Barrett, 2018; Poulsen, 2014). The United States government itself has funded encryption technologies such as Signal and Tor as part of its internet freedom agenda, and the State Department has promoted the use of Tor as a censorship circumvention tool (Harris & Hudson, 2013). However, the United States has also tried to weaken and subvert encryption standards to increase its technical cyber capabilities. While the State

Department was training dissidents in other countries to hide from their governments by using Tor, the NSA was secretly trying to break Tor's encryption and de-anonymise its users (Gellman, Timberg, & Rich, 2013). Other US government agencies, such as the Federal Bureau of Investigation (FBI), have tried to weaken encryption by attempting to mandate the introduction of flaws (or "backdoors") into encryption standards (Savage, 2018; Timberg & Miller, 2014). Most damagingly, the NSA tried to subvert encryption standards used across the internet by encouraging the adoption of a weakened cryptographic implementation as an industry standard (Perlroth, Larson, & Shane, 2013). It then paid US$10 million to the security firm RSA to embed this weakened standard in its products (Menn, 2013).[88]

The tension between network security and offensive cyber capability also arises in the context of the US policy of stockpiling zero-day vulnerabilities. Zero-days are the most carefully guarded secrets in the cyber domain, and so it is difficult to speak of this issue with any specificity. However, it has been clear for many years that the United States government has a policy of stockpiling its most valuable zero-days, rather than disclosing them so that they can be patched by the relevant software developer. The United States' zero-day stockpile has allowed it to create remarkably sophisticated malware platforms such as GrayFish, Flame, QuantumInsert, and Stuxnet. However, by failing to disclose zero-days when it discovers them, the United States government runs the risk that other states or criminal hackers will independently discover the same vulnerability and use it against Americans. A RAND Corporation study estimates that in any given year, a stockpiled zero-day has a 5.7% chance of being discovered by someone else (Ablon & Bogart, 2017, p. 43). This implies that if a state possesses a stockpile of 100 zero-days and attempts to hold on to it for a 10-year period, approximately 43 zero-days in the stockpile would be independently discovered by other actors before the period is over. Thus, its policy of zero-day stockpiling effectively means that the US government has deliberately left American businesses, consumers, and civilian government agencies vulnerable to being hacked.

American policymakers are aware of this trade-off and they have tried to find ways to mitigate it. In 2008, the White House created a Vulnerabilities Equities Process (VEP) to formalise the process of deciding which vulnerabilities the United States should disclose, and which vulnerabilities it should retain for stockpiling or exploitation (Joyce, 2017). The VEP brings together a variety of different

[88] The United States has a long history of attempts to weaken cryptography. During the Cold War, it took the extraordinary step of creating a CIA-controlled front company, Crypto AG, to sell flawed cryptographic equipment to foreign governments (G. Miller, 2020).

intelligence agencies and cabinet departments to weigh the defensive benefits of disclosure against the offensive benefits of retention (United States of America, 2017). Unofficially, the main criteria informing the decision to stockpile or disclose is the so-called NOBUS ("nobody but us") criteria. In other words, the United States discloses most of the vulnerabilities it discovers, but it stockpiles vulnerabilities that it believes are inaccessible to other state actors – for example, because they possess less computational power than the United States (Buchanan, 2017b, p. 2).

The underlying logic behind the NOBUS principle seems plausible, and the NSA claims that it discloses 91% of the vulnerabilities it discovers (NSA, 2015). Michael Daniel, a cyber security advisor to the Obama Administration, states "[t]he idea that we have these vast stockpiles of vulnerabilities stored up – you know, *Raiders of the Lost Ark* style – is just not accurate" (Zetter, 2014c). This claim is supported by some researchers, such as Healey (2016). However, the VEP – like all US policymaking on cyber security – is heavily influenced by the NSA, which has strong institutional incentives to keep the most destructive vulnerabilities for its own use (Schwartz & Knake, 2016, p. 15). This, combined with several high-profile failures, has caused many observers to be sceptical of the VEP's ostensible bias towards disclosure (Schneier, 2016a). One possible failure was "Heartbleed", a flaw in the popular OpenSSL cryptographic library that is used by many websites to send and receive encrypted information (Durumeric *et al*., 2014, p. 475). Heartbleed affected roughly half a million websites at the time of its discovery and was described as one of the worst security lapses in the history of the Internet (Schneier, 2014). Bloomberg News reported that the US government had known about Heartbleed for two years and had used the bug to collect passwords and other useful information rather than disclosing it to the developers of OpenSSL (Riley, 2014), although this was denied by the NSA (Sanger & Perlroth, 2014).

In some cases, exploits that were stockpiled by US intelligence agencies have been leaked directly to malicious actors. In 2016, many of the NSA's hacking tools were stolen by the Shadow Brokers and released onto the internet where they could be freely downloaded by criminals. In October 2017, WikiLeaks published a huge cache of exploits stolen from the CIA, capable of compromising a broad array of devices, which it dubbed the "Vault 7" release (WikiLeaks, 2017). Together, the Shadow Brokers incident and the Vault 7 leak underscored the inherent difficulty of storing software exploits in safety. As the WikiLeaks (2017) press release accompanying the Vault 7 leak points out: "Cyber 'weapons' are in fact just computer programs which can be pirated like any other... they can be copied quickly with no marginal cost." In the aftermath of the leak, the NSA and the CIA tried to determine whether they had been hacked or whether the exploits had been leaked by an insider

(Shane *et al*., 2017). A scathing internal report blamed the CIA for poor operational security and a strategic culture that prioritised cyber offence over defence (Nakashima & Harris, 2020).

It did not take long for other malicious actors to begin using these exploits to wreak havoc. Two weeks after the fifth Shadow Brokers data dump, security researchers estimated that the leaked exploits had been used to infect 200,000 computers around the world (O'Neill, 2017a). The most damaging exploit released by the Shadow Brokers was EternalBlue, an exploit for Microsoft Windows that quickly became the go-to tool for anyone wishing to create malicious software. EternalBlue was immediately adopted by cyber criminals as well as Iranian and Russian APTs (Newman, 2018). In May 2017, it was used to power the WannaCry worm, which infected 230,000 computers across 150 countries, and was subsequently attributed to the government of North Korea (Nakashima & Rucker, 2017). WannaCry's most high-profile victim was the British NHS, which suffered the financial equivalent of £92 million in damage (DHSC, 2018, p. 14). In response to the attack, Microsoft issued an unusually caustic statement blaming the US government, stating that the attack was "yet another example of why the stockpiling of vulnerabilities by governments is such a problem" (Smith, 2017). One month later, EternalBlue was one of two exploits used in the NotPetya malware attack against Ukraine, which was even more destructive than WannaCry. One of the collateral victims was the Danish logistics company Maersk, which had the effect of disabling roughly one-fifth of the world's container shipping capacity, thereby disrupting business supply chains around the world (Greenberg, 2019, pp. 151-153). The US government subsequently valued the total global financial cost of the attack at US$10 billion, making this the costliest malware infection in history by a considerable margin (Greenberg, 2019, p. 199). All of this could have been avoided if the NSA had simply disclosed the underlying vulnerability sooner.

5.4.2 Commercial Trade-Offs

The aggressive use of technical cyber power by the United States government also had the unintended effect of harming US commercial interests. When reports of the NSA's Prism surveillance programme were first leaked, initial media reports incorrectly suggested that the programme gave the NSA unfettered access to the servers of technology companies without the need for a warrant, resulting in an immediate consumer backlash (Levy, 2014). American online services firms and cloud storage providers, such as Amazon, Google, Facebook, and Microsoft, are particularly vulnerable to the perception that their servers have been compromised by US intelligence. Cloud-based software is inherently reliant on consumer trust – individuals and businesses are unlikely to place their private data in the cloud unless they have confidence that the storage provider will employ strong cyber

security practices and keep their private data secure (Zajko, 2018, pp. 46-47). This trust is undermined by intelligence leaks, such as the Snowden revelations, which suggest that internet users who rely on American software companies might end up in an NSA database (Lyon, 2014, pp. 4-5).

The post-Snowden backlash was intensified by President Barack Obama's (2013) clumsy and parochial attempt to defend the Prism programme, in which he stated that "[w]ith respect to the internet and emails, this does not apply to US citizens and does not apply to people living in the United States". This was not a source of comfort to the billions of Google, Facebook, Amazon, and Apple customers who live outside of the United States. The direct costs of the consumer backlash are difficult to measure, but a report by the New America Foundation found that multiple American technology companies reported sales losses after Snowden revealed the scope of the NSA's surveillance operations (Kehl, Bankston, Greene, & Morgus, 2014, pp. 10-11).

The Presidential Commission report commissioned by the Obama Administration to focus on the issue of NSA surveillance agreed that the aggressive use of technical cyber power by the United States would likely harm US commercial interests (Clarke *et al*., 2014, pp. 210-216). Even General Keith Alexander, the director of the NSA at the time of the Snowden leaks, admitted that the NSA's actions had the potential to harm US commercial interests. In an interview with Wired Magazine, he struck an apologetic tone towards US technology companies:

> This isn't the companies' fault. They were compelled to do it. As a nation, we have a responsibility to stand up for the companies, both domestically and internationally. That is our nation's best interest. We don't want our companies to lose their economic capability and advantage. It's for the future of our country. (Alexander, quoted in Levy, 2014)

In response to the Snowden revelations, governments outside of the United States have increasingly put in place policies to limit the reach of US surveillance, which often have the effect of raising the cost of doing business. Several countries – including Russia, Brazil, and Germany – either passed or considered passing "data localisation" laws, which would force internet companies operating within those territories to store user data locally (Chander & Lê, 2015). More recently, the European Union passed the General Data Protection Regulation (GDPR), which contains strong protections for individual privacy as well as some data localisation provisions. Rossi (2018, p. 106) argues that

European outrage over US surveillance led directly to the European Union's decision to pass the GDPR, and that the law would probably not have passed in the absence of the Snowden revelations. Regulations such as data localisation rules and the GDPR have created significant compliance costs for US technology companies. According to one industry estimate, the 500 largest corporations in the United States spent a combined $7.8 billion to comply with the GDPR (Khan, 2017). The most extreme form of "localisation" is the Chinese policy of simply barring US internet companies from its domestic market altogether. As a result, US online services such as Google, Facebook, and Twitter have been excluded from a huge potential market, paving the way for Chinese competitors such as Baidu, Weibo, and WeChat (Yuan, 2018). China has several reasons for this policy – including economic nationalism, and its desire to exclude pro-Western ideas from its domestic information market – but the threat of NSA surveillance serves as a convenient justification for the policy (Arsène, 2016, p. 31; Cendrowski, 2015).

5.4.3 Balancing and Retaliation

The aggressive use of technical cyber operations by the United States has resulted in pushback, resistance, and retaliatory cyber operations from other states. In the aftermath of the Stuxnet attack, for example, Iran carried out a series of cyber operations against the United States and its allies. In 2012, Saudi Aramco, the world's largest corporation, and a key component of the global energy supply chain, suffered a major malware attack on its business network.[89] The malware, which was given the codename Shamoon, wiped the data from more than 30,000 computers and replaced it with an image of a burning American flag (Perlroth, 2012). E. Kaspersky (2017) has identified similarities between Shamoon and malware used against other targets in the Middle East, and FireEye has linked the attacks to an Iranian APT known as "Elfin Team" or APT33, strongly suggesting that the attack was a response to Stuxnet. The attack against Saudi Aramco was followed up in 2013 by a series of DDoS attacks against American banks, which the US government attributed to the Iranian Revolutionary Guard (Perlroth & Hardy, 2013). One of the Iranian hackers gained access to the control system of a small dam in New York; although the dam's sluice gate was not opened, the incident showed that Iranian hackers have the ability to penetrate industrial control systems (Joseph Berger, 2016).[90] Iranian hackers also launched an operation against The Sands, a Las Vegas casino

[89] The malware was, however, unable to move from the Saudi Aramco's business network to its industrial control network, which significantly limited the damage it was able to inflict.

[90] It should be noted that the dam in this hacking incident (the Bowman Avenue Dam, located in a New York suburb) did not pose a significant threat to the surrounding area. The dam is very small, and its sluice gate had been manually closed for maintenance and thus could not be opened electronically. Furthermore, there is no evidence that this is what the hackers actually intended to do (R. M. Lee, Assante, & Conway, 2016b, pp. 4-7).

owned by billionaire businessman, Sheldon Adelson, who had repeatedly called for the United States to adopt a more pro-Israel foreign policy (Elgin & Riley, 2014). These operations were probably a signalling effort intended to deter the United States and its Middle Eastern allies from carrying out further cyber attacks against Iran. However, the Iranian attacks inflicted little lasting damage and one imagines that the deterrent effect was minimal.

Other states that feel threatened by US actions in the cyber domain have responded with soft balancing tactics: forming coalitions with like-minded states to frustrate, delay, and isolate the United States internationally. Between 2012 and 2014, Russia and China were able to temporarily mobilise a large coalition of states in opposition to the multistakeholder system of internet governance, which the United States has historically supported. At the 2012 World Conference on International Telecommunications, 89 states supported this position, while the United States and 54 of its supporters abstained; a result that Klimburg (2017, p. 108) describes as a "stunning success" for the Russo-Chinese bloc. In the aftermath of the Edward Snowden revelations, the United States faced massive diplomatic pressure to make concessions on the internet governance issue. To protect the multistakeholder system, the United States announced in 2014 that it would transfer IANA's functions to ICANN, thus moving the system of internet governance outside of its direct control (Finley, 2016). This was not a major concession; nevertheless, it is significant that American overreach on the issue of surveillance led to subsequent US concessions on the issue of internet governance.

5.5 Explanatory Variables

We now turn to the analytical task of explaining why the United States has adopted this strategy. The United States could have chosen a different strategy, which would have entailed a different set of trade-offs. For instance, the United States could have opted for a Brazilian-style strategy and refrained from carrying out aggressive hacking and surveillance operations. In this counterfactual world, the resources the United States devotes to breaking encryption and exploiting software vulnerabilities might have been devoted to strengthening encryption and fixing those vulnerabilities. Such a strategy would have been less likely to trigger pushback and balancing behaviour by other states and would have enhanced the security of its domestic networks. Alternatively, the United

---

This puzzling choice of target caused some experts to wonder whether the hackers might have intended to attack a different industrial control system, and instead penetrated the Bowman Avenue Dam by accident. Others speculate that the incident might have been an attempt to signal Iranian capabilities to the United States in a low-risk setting that would not provoke an American response (Sanger, 2016c).

States could have chosen to complement its aggressive technical cyber operations with an equally aggressive and destabilising approach to persuasive cyber power. For example, the United States could have chosen to flood the social networks of other states with disinformation campaigns, seeking to undermine overseas political actors it regards as hostile to its interests. And yet, the United States has not opted for either of these possible alternative strategies. Why is this?

As is the case with Brazil, several potential explanations for the US strategy can be pre-emptively rejected. The evidence presented in this chapter suggests that variables such as the psychological traits of the president or the ideology of the current ruling party have little explanatory leverage. This chapter examines US cyber operations during the administrations of four different presidents – George W. Bush, Barack Obama, Donald Trump, and Joe Biden – with divergent leadership styles, psychological attitudes, ideologies, and party affiliations. During this period, there were some changes to American cyber strategy: for example, the United States' use of technical cyber power became significantly more aggressive after the 9/11 attacks and during the war in Iraq; furthermore, the United States seems to have weakened its commitment to its traditional internet freedom agenda during the Trump presidency. Apart from the latter, however, these shifts do not cleanly map onto the transitions between different presidential administrations. Other aspects of US cyber strategy remained broadly consistent throughout this period.

Many authors explain American cyber strategy as being the product of domestic institutions and bureaucratic political factors that are consistent across presidential administrations. For example, Clarke and Knake (2010) generally explain strategic choices with which they disagree (for example, underinvestment in cyber defence, bias toward cyber offence, and failure of the government to regulate cyber security standards) as being the result of short-sightedness on the part of the US intelligence community and a domestic political system that allows corporations to wield too much influence in the political process. F. Kaplan (2017) suggests that US cyber strategy has been produced by tensions between competing interests within the US government and its security community: presidents and public officials who take an interest in the issue; bureaucracies that resist reform; competing groups within intelligence agencies that develop specialisations around particular technologies; intelligence agencies to protect their bureaucratic turf, and so on. Segal (2017, p. 38) argues that the US intelligence agencies are characterised by a strategic culture of "rapaciousness", which has provided the United States with the technical capability to carry out cyber operations as well as "the political will and creativity to use them".

Weber (2018) argues that US cyber strategy is not well integrated with its broader grand strategy. He points out that the country's various policies – carrying out cyber attacks, encouraging the growth of the technology sector, supporting multistakeholderism in internet governance, the internet freedom agenda – are a confusing and conflicting mix that do not add up to a coherent national strategy. This aligns with the argument presented in this chapter, which similarly argues that US cyber strategy is, in many respects, self-contradictory. Weber (2018, pp. 251-253) suggests that this represents a failure of planning and that the United States could have developed a more coherent strategy if it wished to. He criticises the US for its failure to define its approach to the cyber domain with a coherent strategic narrative in the same way that, for example, the strategy of containment defined the US approach to the Cold War.

The most extreme version of this bureaucracy-centred viewpoint is the argument that the NSA and other intelligence agencies constitute a "deep state" that is engaged in a conspiracy against the public. However, a more moderate version of this critique has been advanced by civil libertarians and activists, including Glenn Greenwald (2013) and Edward Snowden (2019). However, one potential problem with explanations that rely on the political intelligence agencies as domestic actors is that it is difficult to find evidence that US cyber power has ever been used to achieve domestic political ends. Zajko (2018, p. 43), a sharp critic of NSA surveillance, nevertheless notes that "[t]he Snowden documents have not shown evidence of domestic abuses of power on the scale disclosed through the Church Committee's investigation of the NSA's activities in the 1960s and 1970s, when the agency was targeting domestic political activity". The presidential commission appointed to investigate the NSA in the aftermath of the Snowden leaks, which included civil libertarians and prominent critics of the intelligence community, found "no evidence of illegality or other abuse of authority for the purpose of targeting domestic political activity" (Clarke *et al.*, 2014, p. 79). To be sure, the Snowden leaks did reveal a culture of secrecy and overreach that could be abused; it is not necessarily wise for the United States to vest so much technical capability, legal authority, and computational power in the hands of a single agency such as the NSA. Nevertheless, these findings suggest that we need to look outside of domestic interests for a satisfying causal explanation of the United States' choice of cyber strategy.

This brings us to state-level rational choice approaches, which emphasise the interests of the United States as a unit rather than its internal domestic actors or intelligence bureaucracies. Notable examples of this approach include the work of Buchanan (2017a, 2020), who argues that the aggressive use of computer hacking by states such as the United States is, to some extent, inevitable

in an anarchic world where states have an interest in signalling, coercion, and cyber defence. Valeriano *et al.* (2018) similarly argue that the United States has adopted its chosen cyber strategy primarily due to the country's position as a global superpower, and its desire to signal its intentions to adversaries while deterring cyber attacks by adversaries. Another example of this approach is the work of Schneider (2020), who applies a rational choice framework specifically to the question of whether the United States should "defend forward" by pre-placing malware in other states' critical infrastructure systems of other states before the onset of a possible conflict.

One notable problem with these rational choice explanations is that none of them provides a clear and satisfying explanation for the apparent reluctance to make aggressive use of persuasive cyber operations. This chapter demonstrates that the United States has exhibited a fair degree of self-restraint in this area: it generally does not make use of large-scale disinformation campaigns, even though it possesses the capability to do so. However, most of the literature that adopts a rationalist perspective is focused exclusively on the use of technical cyber operations and generally does not attempt to explain its approach to persuasive cyber power.

This study attempts to resolve these problems by hypothesising that the apparent inconsistencies and contradictions in US cyber strategy stem from a complex mixture of structural variables from which the United States cannot entirely escape. Like most scholarship in the rational choice school, this study argues that there is a link between a state's approach to cyber strategy and its external security requirements. Furthermore, to explain its approach to persuasive cyber power, this study suggests that this explanation must be modified with an understanding of the preferences of the United States with respect to international institutions.

5.5.1 High External Security Requirements

The United States of America was a minor regional power when it was first established. However, it expanded through a combination of wars and territorial purchases until it came to dominate its continent (Mearsheimer, 2003, p. 76). In 1823 it issued the Monroe Doctrine, signalling its desire to establish hegemony over the entire Western hemisphere (Lake, 2006, p. 26). It fended off a secessionist from its southern states between 1861 and 1865, thus ensuring that it would have no peer competitors within its region (P. Thompson, 2007, p. 129). By the twentieth century, it had become so powerful that it was able to turn its attention abroad, waging overseas wars in Europe and Asia to prevent the rise of hegemonic powers in other regions (Mearsheimer, 2003, p. 76). By 1945 it had become the world's dominant economic power, and after the collapse of the Soviet

Union in 1991, it was left as the only hegemonic state in any region of the globe (Cohen, 2004, p. 52; Fukuyama, 1989). Although it is generally believed that the international system is currently trending towards multipolarity, the United States remains the most powerful state in the world in absolute terms (Mearsheimer, 2018, p. 4; Nye, 2015, pp. 7-8; Zakaria, 2011, p. 34).

This might seem to imply that the United States is very secure, and indeed, there is no single state that could pose a conventional military threat to it. Nevertheless, the United States faces high external security pressure. However, while the United States has enormous resources with which to pursue its foreign policy goals, it also has a vast set of interests to defend. Its economic wealth is sustained by a complex international network of trading routes, commercial partners, financial linkages, and international institutions (Ikenberry, 2011, p. 2; Kindleberger, 1973, p. 307; Krasner, 1976, pp. 337-338). To protect these interests, the United States has taken on increasingly expensive security commitments, accepted large numbers of allies and client states, and diverted a significant portion of its economic resources to its military. Between 2005 and 2022, the United States spent an average of 3.95% of its GDP on its military, compared to a global average of 1.93% (SIPRI, 2022). Vine (2015, p. 6) calculates that the United States possesses nearly 800 overseas military bases or installations; by contrast, Russia only has 21 overseas military bases (Goble, 2019), and China currently has only one (Cabestan, 2019, p. 6). Maintaining an overseas military presence on this scale is extraordinarily expensive; as a result, the United States is constantly confronted by the problem of "imperial overstretch" articulated by Kennedy (1989).

One side effect of the high external security pressures facing the United States is its surprisingly poor performance in major wars. The United States fought numerous wars during the twentieth and twenty-first centuries, usually to protect its client states or to prevent the rise of competing hegemonies in other regions (Mearsheimer, 2003, pp. 140-141). However, despite its massive advantages in technology and matériel, the United States has achieved only two decisive military conflicts since 1945: its victory over Iraq during the 1990-1991 Gulf War, and its defeat of Serbia during the 1998-1999 Kosovo War. It achieved a mixed result in the 1950-1953 Korean War, and became embroiled in long-running, unsuccessful counterinsurgency conflicts in Vietnam, Iraq, and Afghanistan.[91] This mixed record of military success does not stem from a lack of material power; instead, it reflects the inherent difficulty of coping with security challenges that are global in scope.

[91] This military record is an interesting contrast with Brazil's military record, which is discussed in Chapter Four of this study. Although Brazil is a much weaker power than the United States, it has managed to achieve a higher success rate in war, in part because it has more freedom to choose which conflicts it wishes to enter.

As we have seen throughout this chapter, the United States is a quasi-hegemonic power in the international system, capable of mobilising huge reserves of military and economic power in pursuit of its foreign policy goals. Nevertheless, the scale of US interests and commitments around the world has stretched even these vast resources thin. This structural disconnect between ends and means is, of course, a perennial problem for all powerful states with wide-ranging interests (Brighi & Hill, 2016, p. 159). The basic contours of the problem would have been familiar to the strategists of the Roman Empire, for example (Luttwak, 1979, p. 191). Thus, the United States is under continuous pressure to find new, unconventional, and inexpensive methods for advancing its foreign policy interests. These external security pressures have acted as the primary determinant of the United States' aggressive pursuit of technical cyber power.

Indeed, there is a clear relationship between the external security pressures facing the United States and its increasing use of technical operations as a tool of foreign policy. It is not a coincidence that the war on terror was also the historical period in which cyber operations became a routinely used tool of US foreign policy (F. Kaplan, 2017, pp. 145-160). The United States has shown few moral qualms about killing suspected terrorists (Price, 2012, pp. 9-10), but to do so, it first needs to identify and locate targets (Valeriano *et al.*, 2018, p. 194). Since the conflict with terrorist groups is asymmetric and relies on intelligence gathering rather than overwhelming force, this has given US cyber operations a strong focus on espionage. In this sense, cyber operations have served to complement traditional military operations (Moltke, 2019).

It was the Iraq War, in which the United States came close to a military catastrophe during 2006 and 2007, that directly led to the RT-RG programme and the NSA's move from targeted end-point collection to a system of "collecting the whole haystack". External security pressures, in the form of terrorism fears in the decade after 9/11, led to the passage of the Protect America Act and the subsequent creation of the NSA's "Turbulence" programme, in which it sought to apply the RT-RG philosophy at a global scale. The United States' concerns over nuclear proliferation and its desire to avoid a destabilising war between Iran and Israel during a period when its military was severely overstretched led directly to the development of Stuxnet – the first malware attack that inflicted physical damage on a nation's critical infrastructure. American policymakers were well aware of the potentially destabilising effects of Stuxnet. General Michael Hayden, Director of the NSA under George W. Bush, stated that the attackers had "crossed the Rubicon", and that worried that "in one sense at least, it's August 1945" (Sanger, 2012b). However, when faced with the prospect of a destabilising regional war between Israel and Iran, and torn by competing military demands in Iraq

and Afghanistan, neither George W. Bush nor Barack Obama gave serious thought to abandoning the operation (Sanger, 2012c).

In the following years, the desire to slow down North Korea's missile programme may have led the United States to adopt similar tactics against that country, albeit with less success. In 2015, the United States was fearful of the threat posed by the Islamic State – but it had to balance this threat against competing foreign policy priorities across the world and was in no mood to launch yet another war in the Middle East after fighting the war on terror for 14 years. As a result, the United States looked for non-conventional methods of attacking the Islamic State, including cyber operations (Stern, 2015, pp. 64-70). Meanwhile, the resumption of great power competition against a rising China and a revisionist Russia spurred the development of the suite of staggeringly sophisticated malware associated with the Equation Group. In short, whenever the United States has been faced with tricky or inconvenient foreign policy problems, American policymakers have instinctively reached for any tool that seems to offer a low-cost solution – and over the last two decades, this has frequently included technical cyber operations. This pattern has occurred consistently, regardless of the president or party that happened to occupy the White House. Over time, the cumulative effect of such policy choices – usually made in response to particular circumstances rather than according to any grand plan – has pushed the United States toward the "technical-aggressive" cyber strategy outlined in this study.

5.5.2 Positive Institutional Preferences

In light of its high external security requirements, it is reasonable to ask why the United States has not used persuasive cyber power more aggressively. In particular, why has the United States not made a concerted effort to disseminate disinformation and subversive narratives within the social networks of its many adversaries? The closest the United States has come to using persuasive cyber power in this way was the short-lived cyber campaign conducted by the CSCC under Alberto Fernandez, which aimed to exploit the phenomenon of memetic transmission. However, this persuasive cyber campaign proved to be controversial and it was swiftly abandoned. Moreover, even in this case, the United States opted for overt rather than covert execution, effectively reducing the campaign's effectiveness voluntarily. To explain why the United States has made this strategic choice, we must consider the second dependent variable: the United States' institutional preferences. With some reservations, the United States can be viewed as having "positive" institutional preferences, in the sense that it focuses mainly on maintaining institutions that benefit its interests, rather than undermining institutions that do not align with its interests.

These institutional preferences stem from the United States' historical role in shaping numerous international institutions that currently organise global politics. In the aftermath of World War II, when its power was unparalleled, the United States led the construction of a set of institutions reflecting its political preferences. Consequently, the United States embedded many of its preferred norms and interests within the governance architecture of the international system. Although American enthusiasm for international institutions has varied under different presidential administrations, organisations like NATO have consistently served as a key conduit through which the United States exerts influence on the international system. This institutional framework has not only helped legitimise the United States' quasi-hegemonic position in the global arena but also enabled it to maintain this status without inciting a military balancing coalition against it, a feat rarely achieved by powerful states (Lieber & Alexander, 2005, pp. 119-125).

These institutions exist in both the security and economic spheres. In the security sphere, the United States has established an institutionalised system of permanent alliances. This system originated in 1949 with the signing of the North Atlantic Treaty and later expanded to include mutual defence pacts with Australia (1951), the Philippines (1951), South Korea (1953), and Japan (1960) (Beckley, 2015, p. 23). The system outlasted the Cold War and has now been in existence for so long that it is easy to lose sight of how novel and unusual this is. Previous great powers have utilised local allies and auxiliaries to assist in their overseas wars and formed ad hoc alliances with other great powers. However, these alliances were typically seen as temporary partnerships. Lord Palmerston's belief that a great power such as Britain should have "no eternal allies" (Parliament, 1848) is often regarded as a classic expression of nineteenth-century European *realpolitik* (Heath, 1969). The United States has ignored this principle and instead entered into long-term commitments, thus creating strong security partnerships with its allies. Through this policy, the United States effectively transformed important regions of Europe and Asia into voluntary protectorates (Brzezinski, 2013, p. 12).

The United States has pursued a similarly innovative programme of institution building in the economic sphere. After World War II, it played a key role in creating the Bretton Woods institutions: the IMF, which oversees international finance and acts as a lender of last resort, and the World Bank, which oversees international development (Steil, 2013, pp. 127-128). It also played an important part in the negotiations that led to the General Agreement on Tariffs and Trade (GATT) and its successor, the WTO. These economic institutions serve several functions that benefit the United States: they enable American firms to trade and operate globally, protect American investors

and intellectual property rights in overseas markets, and provide access to international capital markets for the United States.

Although the United States generally holds positive institutional preferences, these preferences are neither consistent nor strong. Some international institutions have been targets of American hostility, particularly during periods of Republican governance. The United States has long complained that the UN General Assembly is biased against itself and Israel; it opposed the International Criminal Court (ICC) and even threatened to invade the Netherlands if any of its service members were to be prosecuted there; it chose not to sign the Ottawa Treaty against anti-personnel landmines; and it even refused to ratify the UN Convention on the Law of the Sea, a treaty that most experts believe would be beneficial for US economic and geopolitical interests (Wahal, 2022). However, none of these treaties or agreements holds the same level of importance as institutions such as NATO and the WTO. Thus, the United States has significantly more at stake in the current institutional *status quo* than it would have to gain by disrupting it. When considering the most important international institutions, US preferences can therefore be described as "positive", even if the rhetoric from its elected officials does not always perfectly reflect this.

These positive institutional preferences help explain why the United States has not used persuasive cyber power more aggressively. This study argues that persuasive cyber power is an offence-dominant technology: It is useful for undermining trust in institutions, but not for supporting existing institutions or creating new ones. For example, if China were to establish a NATO-like alliance that the United States perceived as a threat, then we might expect the United States to use persuasive cyber power to undermine trust in this alliance among the populations of its member states. However, since no such target currently exists, the potential payoff of using persuasive cyber power is relatively small. Furthermore, aggressive use of persuasive cyber operations would further increase the costs and trade-offs of America's already costly cyber strategy, as these operations could backfire and reduce social cohesion and trust in the domestic information market. Thus, when considering whether to use persuasive cyber power, the United States finds itself in a similar position to Brazil: the potential payoffs are low, making it rational to avoid the potential trade-offs.

However, the theory presented in this study suggests that if the United States' institutional preferences were to shift, perhaps due to a desire to exit the post-World War II institutional order it helped design, or because rival powers created new and threatening international institutions, the USA's strategic approach to persuasive cyber power would change accordingly. Chapter Seven of this

study discusses potential scenarios for the future of American cyber strategy and considers how such scenarios might unfold. For now, it is worth noting that there has already been a small-scale test case of this hypothesis.

The Trump Administration, in power from 2017 to 2021, exhibited an unusually strong hostility toward international institutions, even when compared to previous Republican administrations. It sought to renegotiate or end US participation in major institutions such as the TPP, NAFTA, the WTO and even NATO (Bown & Irwin, 2019). Trump's Secretary of State, Mike Pompeo, sharply criticized the EU, IMF, and World Bank, stating that international organisations that do not advance the security and values of the United States and its allies "must be reformed or eliminated" (Pompeo, 2018). Trump himself expressed his hostility toward international institutions while speaking before the UN General Assembly, proclaiming: "The future does not belong to globalists. The future belongs to patriots" (Trump, 2019).

Trump's policies on international institutions appear to have reflected his longstanding personal views on foreign policy, which differ significantly from the American political establishment. As early as 1990, in an interview with *Playboy magazine*, Trump argued that the United States was "being ripped off so badly by so-called allies" and stated that Japan, Germany, Saudi Arabia, and South Korea were "making billions screwing us" (Trump & Plaskin, 1990). However, the Trump Administration's policy on institutions can also be seen in structural terms, as a response to the relative decline of US hegemony and the fear that rising powers like China might create new institutional frameworks that serve to constrain rather than enable the United States. The theory of cyber power presented in this volume predicts that if US preferences start to shift in this way, its approach toward persuasive cyber power should shift in tandem.

Indeed, this is what happened. As this chapter notes, the approach of the Trump Administration to persuasive cyber power differed significantly from its predecessors. Under USAGM CEO Michael Pack, the United States' international media agencies deviated from traditional journalistic norms and became more overtly propagandistic; the United States abandoned many anti-censorship technologies previously funded through the Open Technology Fund; the CIA successfully sought permission to carry out "hack and dump" operations; and Trump used his personal Twitter feed to threaten other states and criticise international institutions. Collectively, these steps can be understood as a partial shift in US cyber strategy, corresponding with the partial shift in US institutional preferences. However, the Trump Administration was in power for only one term, and

these shifts have been partially reversed under Trump's successor, Joe Biden. It remains to be seen whether this anti-institutional shift that occurred under Trump was merely a temporary departure from the norm, or whether it will mark the start of a long-term adjustment in US strategy. This question is beyond the scope of this study. However, if the United States is indeed beginning a long-term shift toward negative institutional preferences, it will have strong incentives to realise those preferences through the use of persuasive cyber power.

5.6 Conclusion

This chapter argues that the United States' cyber strategy is shaped by its external security requirements and its institutional preferences. As a regional hegemon, the United States faces a broad array of security challenges that demand attention and resources, which cannot be solved through conventional military means. At the same time, the United States holds positive institutional preferences that stem from its historical role in the development of the liberal international order. These two imperatives interact in complex ways to produce the country's "technical-aggressive" cyber strategy. As such, the case of the United States is congruent with the theoretical expectations of this study.

The United States is a regional hegemon with a defensible geography, a large and dynamic economy, and a well-funded military. However, the global scale of its interests, combined with the multiplicity of threats and adversaries, ensures that it continually faces new foreign policy challenges and crises that compete for its finite attention and resources. In the decades after 2000, the United States engaged in a global conflict against non-state actors such as Al Qaeda and ISIS, was deeply concerned about the danger of nuclear proliferation by states like Iran and North Korea, and sought to balance against the rising power of China and the territorial ambitions of a revanchist Russia. Unable to achieve all of these goals through conventional means, successive presidential administrations chose to vest significant legal authority and vast computational power in the country's intelligence agencies, especially the NSA. The US intelligence community then used this power to construct extensive surveillance systems, sabotage the nuclear programs of other states, and engage in long-running cyber conflicts with Russia and China. Thus, the United States' aggressive use of technical cyber power can be seen as a direct response to the external security pressures it faced during this period.

At the same time, the United States is part of an extensive system of alliances and institutions that promote its interests. The United States is the architect of the world's most powerful military

alliance, NATO. It was also a key actor in the creation of global economic institutions, such as the World Bank and the WTO, which have established the capitalist model of economic development and international free trade, both of which the United States tends to favour. The United States' commitment to institutional rules is inconsistent, and these international institutions are a frequent target of populist criticism from domestic political actors. However, if we set aside these internal critiques and view the United States within its broader strategic context, it becomes clear that the country does not currently face any institutions or alliances that are sufficiently hostile or threatening that they would warrant being targeted with a disinformation campaign. Therefore, much like Brazil, the United States has rationally refrained from carrying out such campaigns.

The United States does use other forms of persuasive cyber power: it has conducted overt public diplomacy campaigns, encouraged other states to adopt its preferred model of internet governance, and even sponsored the development of censorship circumvention technologies. However, it has generally done these things overtly rather than covertly, refusing to take advantage of the attribution problem to undermine institutional trust and make its persuasive cyber campaigns more successful. This stands in stark contrast with another actor, the Russian Federation, whose cyber strategy is examined in the following chapter.

Chapter 6
Russia

6.1 Introduction

The Russian Federation has adopted an exceptionally aggressive strategy, involving the extensive use of both technical and persuasive cyber operations. This chapter analyses and explains the underlying strategy that informs Russia's actions in the cyber domain.

Russia makes intensive use of online espionage and sabotage in support of its foreign policy interests. This aggressive use of technical cyber power is, in some respects, similar to the approach used by the United States, as outlined in Chapter Five of this study. There are, however, some important differences in detail. The United States tends to engage in targeted attacks, utilising precise and stealthy intrusions, avoiding civilian targets, usually steering clear of non-discriminating methods such as DDoS attacks, and to date, has not launched cyber attacks on civilian infrastructure targets. In contrast, Russia has conducted cyber attacks against civilian targets, including an election results server in Ukraine, an Estonian bank, news sources in Georgia, and the power grid in Ukraine. On one notable occasion, a Russian malware attack directed against Ukraine inadvertently spread across international borders, infecting the Danish logistics company Maersk and temporarily grounding one-fifth of the world's container shipping capacity.

However, the feature that most sets Russian cyber strategy apart from other states is its aggressive use of persuasive cyber operations. For years, Russia has carried out sustained disinformation campaigns to amplify internal divisions within the United States. It engaged in a targeted intervention during the 2016 US presidential campaign, with the intention of swinging the election to Donald Trump. It has even supported secessionist movements that aim to break up the United States, including movements pushing independence in Texas and California. Russian hackers also seem to have engaged in a targeted intervention prior to the 2017 presidential election in France, intending to swing the election in favour of the far-right candidate Marine Le Pen. Russia probably supported the Leave campaign during the 2016 Brexit referendum in the United Kingdom and amplified the cause of Catalan independence from Spain. Indeed, it seems likely that every major secessionist, Euroskeptic, or anti-NATO political movement in Europe since 2014 has received support from Russian persuasive cyber operations.

This strategy has been enormously costly for Russia, and its adoption has required the Russian state to be exceptionally risk-tolerant. Russia's population, exposed to ceaseless propaganda from the Russian state, has become cynical and distrustful. In comparative studies on societal trust, Russia consistently ranks near the bottom. Russia's cyber strategy has triggered justifiable suspicion in other countries about whether its technology companies can be trusted, thereby frustrating Russian efforts to build a high-technology economy and reduce its reliance on the fossil fuels sector. Furthermore, Russia's aggressive cyber strategy has done immense damage to its overseas reputation, effectively closing off possible avenues of *rapprochement* with the West. Why has Russia selected this costly strategy, instead of other possible strategies? This chapter argues that two key variables explain Russia's strategic choices in the cyber domain: its high external security requirements and its negative preferences regarding international institutions. These two factors have combined in the case of Russia to produce a cyber strategy that would be deemed unacceptably risky by the policymakers of most other states.

6.2 Russia's Use of Technical Cyber Power

Russia is a highly capable state actor in the cyber domain, possessing advanced technical cyber power (Giles, 2016, p. 31). It possesses a military formidable intelligence agency, the GRU (Main Intelligence Directorate), which employs some of the world's most skilled computer hackers. The GRU's offensive cyber units, such as Unit 26165 ("Fancy Bear") and Unit 74455 ("Sandworm"), are responsible for some of the most notorious recorded APT incidents (Greenberg, 2019, p. 243). In addition, Russia also maintains a myriad of other security agencies that are responsible for APT activity, including the FSB (Federal Security Service) and the SVR (Foreign Intelligence Service) (Galeotti, 2016). However, Russian technical cyber operations are distinguished from those of other states by their indiscriminate nature. In the CFR Cyber Operations Tracker (2020), for example, Russia is coded as the aggressor in 152 cyber operations; the second-highest number of any state in the dataset, after the People's Republic of China (CFR, 2022).

The following sections will examine some of the notable examples of Russian cyber operations, to discern the various commonalities and patterns that comprise Russia's approach to cyber conflict. Firstly, Russia has engaged in cyber operations aimed at preserving its influence in the Baltics and the Caucasus, targeting countries that were once part of the Soviet Union and that Russia regards as falling within its sphere of influence. Secondly, it has carried out a sustained cyber campaign against Ukraine. Thirdly, Russia has been engaged in great power rivalry with the United States, employing cyber capabilities to undermine the political stability and security of its main global competitor.

Lastly, Russia has called for "cyber arms control," advocating for global agreements to regulate state behaviour in the cyber domain, which may seem contradictory to its aggressive cyber strategy. The following sections will examine each of these categories of operations in turn.

6.2.1 Preserving Influence in the Baltics and the Caucasus

The three Baltic states of Latvia, Lithuania, and Estonia have been an important source of conflict between Russia and the West during the post-Cold War period. The Baltic republics have traditionally orientated themselves towards Scandinavia and Central Europe rather than Russia; when the USSR began to collapse in 1990, they were among the first Soviet republics to break away (Geron, 1991, pp. 135-136). They quickly began to develop political and economic institutions that aligned with Western European norms and began signalling their desire to join NATO (Banka, 2019). However, NATO membership for the Baltic states was seen as a strategic threat by Russia (Götz, 2015, pp. 8-9). Together with Poland, the Baltic states would allow NATO to fully encircle the exclave city of Kaliningrad, a major Russian military base in the Baltic littoral (Asmus & Nurick, 1996, pp. 124-125). More importantly, from the Russian perspective, NATO membership for the Baltic states could potentially bring Western military forces dangerously close to its geographic heartland, effectively moving the strategic frontier between NATO and Russia to within 150km of Saint Petersburg. In 1997, then-Foreign Minister Yevgeny Primakov summarised Russia's security concerns as follows:

> Russia cannot remain indifferent to the factor of distance – the Baltic countries' proximity to our vital centres. Should NATO advance to new staging grounds, the Russian Federation's major cities would be within striking range of not only strategic missiles, but also tactical aircraft… (Quoted in Donaldson & Nadkarni, 2019, p. 233)

Boris Yeltsin's government attempted to draw a "red line" around the issue of NATO membership but lacked the military or economic tools to enforce it (Black, 1999, p. 251). Yeltsin's successor, Vladimir Putin, followed a different approach in the region. Putin was presumably aware that Russia could not compel NATO to accept its preferences and thus conceded the issue of NATO membership for the Baltics. Instead, Putin chose to focus on pursuing Russia's interests in "core" areas such as Belarus and Ukraine (Radin & Reach, 2017). As a result, Latvia, Lithuania, and Estonia became NATO members in 2004 with only muted Russian protests (D. V. Trenin, 2011, p. 107). Nevertheless, Russia still has important interests at stake in the Baltics; it particularly wishes to discourage the United States from establishing forward military bases in the region. As relations between Russia and NATO have worsened over time, Russia has used a variety of foreign policy tools to destabilise the Baltic

states and signal its resolve to its adversaries. These measures have included provocative shows of military force; economic statecraft; supporting pro-Russian domestic factions within Baltic states, and, since 2007, the use of cyber operations (Götz, 2015, pp. 12-15).

In 2007, Russia engaged in a brief cyber conflict with Estonia. The immediate *casus belli* was Estonia's decision to relocate a bronze statue from the centre of its capital, Tallinn, which commemorated Russian war casualties during World War II. Ethnic Russians (both in Estonia and Russia itself) tended to view the statue as a symbol of sacrifice and heroism during the war. On the contrary, ethnic Estonians tended to see it as a painful reminder of their country's repression during the Soviet period (Schmidt, 2013, p. 175). On 27 April, Estonia's conservative and pro-Western government went ahead with plans to remove the statue, provoking sharp condemnation from Putin (Myers, 2007). That same night, many Estonian websites were vandalised, and Estonian government agencies and news sites began to experience DDoS attacks. During the next four weeks, DDoS attacks increased in scope and intensity, using massive levels of internet traffic from botnets[92] to overwhelm the Estonian government and banking websites (Kostadinov, 2013).

It should be noted that DDoS attacks are inherently unsophisticated, and these attacks did not inflict permanent damage on the Estonian internet (Valeriano & Maness, 2015, p. 145). Over the next four weeks, Estonia was able to secure additional bandwidth and restore online services, and the DDoS attacks died down. However, these operations succeeded in creating a high level of fear and uncertainty within Estonia. Estonia was, and still is, a world leader in its use of the internet to provide government services, which inadvertently increased its vulnerability to denial-of-service attacks (Davis, 2007; Finn, 2007). For Estonians who found themselves cut off from access to government services and their savings, the episode was unsettling, especially since it signalled the hostility of a large and powerful neighbouring state.

The attribution of the attack has remained contested. From the outset, many Estonians suspected that the attacks were orchestrated by Russia (Finn, 2007). However, many security researchers who have investigated the incident believe the attacks were probably carried out by Russian patriotic hackers; private Russian citizens who reacted with outrage at the removal of the statue (Herzog,

[92] A botnet is a group of computers which have been compromised by malware, and are linked together in parallel into a type of distributed supercomputer. Some botnets are very large; the biggest are made up of millions of compromised computers. Once a botnet has been assembled, it can be used for a variety of malicious purposes, including sending out spam emails, cracking passwords, mining cryptocurrency, or carrying out DDoS attacks.

2011, p. 28). Hendler (quoted in Waterman, 2007) argues that the incident was something "more like a cyber riot than a military attack". However, other observers – including government officials in Estonia – suspected the involvement of the Kremlin (Traynor, 2007). Based on a combination of technical and contextual political evidence, Ottis (2008, pp. 166-167) argues that the most reasonable interpretation of the event is that Russian patriotic hackers carried out the bulk of the attacks, but they did so with the consent and tacit encouragement of the Russian government. Certainly, the Russian government did not make any obvious efforts to stop DDoS attacks once they began. Most plausibly, the Kremlin viewed the DDoS attacks as a useful signalling mechanism, through which it was able to convey its ability and willingness to impose costs on Estonia if the latter continued to align itself with the West.[93]

One year after the bronze soldier controversy, another cyber incident occurred in the Republic of Georgia. Like the Baltics, Georgia had long been fearful of its powerful neighbour to the north. After the 2003 "Rose Revolution", which brought pro-Western President Mikheil Saakashvili to power, Georgia tried to allay these fears by pursuing NATO membership. Unlike the Baltics, however, Georgia is located in the Caucasus: a region that is far from Western Europe, and which Russia continues to regard as falling within its natural sphere of interest (Karagiannis, 2013, pp. 83-84; D. Trenin, 2009, pp. 143-146). Russia is implacably opposed to the expansion of NATO in the Caucasus, and it has used every foreign policy tool at its disposal to achieve this end. When NATO granted Georgia a Membership Action Plan in 2008, Russian General Yuri Baluyevsky responded that "Russia will take steps aimed at ensuring its interests along its borders... These will not only be military steps, but also steps of a different nature" (Reuters, 2008a). In Georgia, Russia's most visible strategy has been to support pro-Russian separatists in the provinces of Abkhazia and South Ossetia (Mearsheimer, 2014, p. 79). The NATO policy document on expansion suggests that countries should not be admitted into the alliance if they have unresolved "ethnic disputes or external territorial disputes including irredentist claims, or internal jurisdictional disputes" (NATO, 1995). Russia is, of course, aware of this policy, which gives it a strong incentive to fuel such territorial disputes. In

[93] It should be noted that this signalling strategy was ineffective. The 2007 DDoS attacks did not deter Estonia from pursuing closer alignment with the West, and in fact produced the opposite outcome: in the aftermath of the incident, Estonia developed considerable expertise on cyber security issues, and a NATO cyber defence centre was established in Tallinn. Estonia's perceived expertise on cyber security has allowed it to present itself as an active contributor to the NATO alliance, rather than merely a passive recipient of security (Gold, 2019). However, this unfavourable outcome does not disprove the allegation that Russia was complicit in the 2007 attacks. Certainly, it would not be the first time that a powerful state engaged in foreign policy behaviour that ultimately proved to be detrimental to its own interests.

addition, Russia has used several other foreign policy tools to keep Georgia divided and demoralised, including propaganda and cyber operations.

The first Russian cyber operation against Georgia occurred in the context of the 2008 war. That year, the Georgian government in Tbilisi attempted to forcibly reintegrate the breakaway provinces of Abkhazia and South Ossetia. In response, Russia launched a massive military intervention in these provinces, blockaded Georgia's coastline on the Black Sea, and then invaded Georgia proper (Allison, 2008, pp. 1157-1158). In the build-up to the war, Georgia's government websites were flooded with DDoS traffic, some of which contained the code "win+love+in+Rusia" (Nazario, 2009, p. 167). The effects of the cyber operation paled in comparison with the broader impact of the war but, it serves to illustrate the evolving nature of Russian strategy during this period. By disrupting the ability of the Georgian government to communicate with the world, the attackers complicated Georgia's efforts to present its side of the war to international audiences, allowing Russian narratives about the war to take hold (Greenberg, 2019, p. 95). Eventually, the Georgian government was able to break out of the Russian "cyber blockade" by registering an account on Blogger – a free service provided by Google – to communicate directly with foreign audiences (Korns & Kastenberg, 2009, pp. 67-68). By then, however, the war was effectively already over. Since then, several military strategists have come to regard the 2008 Georgia war as a landmark event, since it was the first occasion in which cyber operations were integrated into a broader combined arms operation (Hollis, 2011, p. 2; White, 2018, p. 1).

The denial-of-service attacks used against Georgia were technically similar to those used previously against Estonia; in this case, there was much stronger evidence suggesting the direct involvement of the Kremlin. Many of the botnets that were used to flood Georgian servers were controlled using "BlackEnergy", a malware platform that is frequently used by Russian state-controlled APTs (Nazario, 2009, p. 177). Throughout the war, DDoS attacks were coordinated from centralised websites (such as "StopGeorgia.ru"), which published target lists that seemed to operate in sync with Russian war planning (Greenberg, 2019, p. 93; Segal, 2016, p. 68). If the earlier Estonian DDoS attacks were spontaneous and unplanned, the lesson that Russia seems to have learned is that DDoS attacks could be a useful foreign policy tool when properly channelled to serve the interests of the state.

In the aftermath of the 2008 war, Russia has continued to engage in periodic cyber operations against Georgia. In 2010 the security firm FireEye published a report on the Russian threat actor "Fancy Bear" (or APT28, in FireEye's naming system), which stated that the group had conducted

cyber espionage operations throughout the Caucasus but was especially focused on Georgia (FireEye, 2014, p. 8). The known targets included the Georgian Ministry of Internal Affairs, the Georgian Ministry of Defence, and a US-based journalist who covered the region (FireEye, 2014, pp. 8-10). In 2012, Georgia's CSIRT, known as CERT-Georgia, announced that it had discovered a targeted malware infection, "Georbot", which seemed to be specifically designed to spy on Georgian agencies, banks, and NGOs (CERT-Georgia, 2011, p. 16). CERT-Georgia provided strong evidence attributing the operation to the Russian government; it even managed to compromise a computer operated by one of the Russian hackers and used its webcam to capture a photograph of him (CERT-Georgia, 2011, p. 22). In October 2019, Georgia experienced another campaign of cyber vandalism: a national television station was knocked off the air, and roughly 2000 Georgian websites were altered to show a photograph of former president Mikheil Saakashvili – Russia's nemesis during the 2008 war – with a caption saying "I'll be back" (BBC, 2019).[94] Four months later, more than 20 countries (including Georgia, the United States, the United Kingdom, Canada, New Zealand, Australia, and several EU states) issued statements attributing the attack to the Russian APT "Sandworm" (Roguski, 2020).

In addition to these high-profile cyber operations against Estonia and Georgia, Russia has also carried out several smaller and less-publicised cyber operations against states within the Baltic region, the Caucasus, and Central Asia. For example, Russia has carried out cyber operations against Lithuania (LRT.lt, 2020; Rhodin, 2008), Kyrgyzstan (Bradbury, 2009), Latvia (Reuters, 2018), Kazakhstan (Cimpanu, 2019), Armenia (Faou, 2020), and Azerbaijan (QuoIntelligence, 2020). These operations vary significantly in terms of their targeting choices, their level of technological sophistication, and their immediate purpose. In terms of technological sophistication, Russian cyber operations in the region range from the simple denial-of-service attacks used against Estonia to the highly advanced malware used by the Sandworm APT. In terms of their immediate purpose, the 2007 DDoS attacks against Estonia served as a signalling mechanism, while the 2008 DDoS attacks against Georgia helped to support Russia's conventional military operations on the ground. Other operations (such as "Georbot") were focused on espionage. Finally, the 2019 mass vandalism of Georgian websites could have served a dual purpose: as a signalling mechanism and as a direct intervention in domestic Georgian politics.

[94] After the 2008 war, Saakashvili served as president of Georgia until 2013. In 2015 he became a Ukrainian citizen and was appointed governor of Ukraine's Odessa administrative region; however, he was stripped of his Georgian citizenship. He is currently facing criminal charges in Georgia, which he claims are politically motivated.

6.2.2 Destabilising Ukraine

The most aggressive and destructive Russian cyber operations during the period covered by this case study are those that have been directed against Ukraine. Russia's efforts to maintain its political influence in Ukraine and to keep European and American influence out have been a central foreign policy objective during the presidency of Vladimir Putin. During the period from 2014 to 2022, in which Russia occupied Crimea and the Donbas, but had not yet committed to a full-scale invasion of Ukraine, Russia made use of a wide variety of non-traditional strategies to destabilise and coerce Ukraine, including cyber operations.

There are several reasons why Russian foreign policy accords such high importance to Ukraine. Many Russians have a romantic attachment to the region, grounded in a sense of shared history and culture (Gvosdev, 2014, pp. 17-18; Kissinger, 2014). Ukraine is the birthplace of the Kievan Rus; it was incorporated into the Russian Empire by Catherine the Great and Grigori Potemkin; it was the scene of Russian military triumphs over invading Swedes, Ottomans, and Nazis. Therefore, it is not difficult to imagine that some Russians view Ukraine as falling within Russia's "natural" sphere of influence. Others see Russia's Ukraine policy as being grounded in either Vladimir Putin's personality (Marten, 2015, pp. 191-192) or Russia's regime type (Motyl, 2015, p. 83). However, realists such as Mearsheimer (2014, p. 82), Götz (2015, pp. 3-4), Larrabee (2010, p. 38), Waltz (2000, pp. 30-32), and Walt (2018, p. 33) argue that Russia has significant security interests at stake in Ukraine and these interests will continue to exist regardless of who occupies the Kremlin. The Crimean Peninsula hosts the Russian naval base at Sevastopol, a vital warm-water port that gives Russia maritime access to the Black Sea and the Mediterranean. Much of Russia's exported natural gas has historically passed through pipelines in Ukraine. Most importantly, Ukraine is seen as a vital buffer between Russia and potential future adversaries. With Ukraine's northern border separated from Moscow by little more than 500 km of flat and indefensible terrain, Russia believes that it is utterly unacceptable for Ukraine to align itself with any state or alliance it considers hostile.

Russia has used a variety of tactics to prevent such an outcome. Before the Euromaidan protests in 2014, Russia attempted to preserve its influence through a combination of economic inducements and support for Russophile parties and candidates in Ukrainian politics. After the overthrow of the pro-Russian president Viktor Yanukovych in 2014, Russia sent troops and materiel to fuel a separatist conflict in the Donets Basin, similar to the "frozen conflicts" in Abkhazia and South Ossetia. Russia's apparent goal was to keep Ukraine weak and internally divided, thereby reducing its attractiveness as a potential NATO member. Furthermore, Russia invaded the Crimean Peninsula in 2014 and then

organised a hasty referendum to legitimise its annexation. This move is perhaps best understood as an insurance policy, designed to ensure permanent Russian control over Sevastopol regardless of future developments in domestic Ukrainian politics. A third element of the Russia strategy from 2014 to 2022 was to weaken Ukraine's economy and social cohesion through a combination of economic statecraft, propaganda, and cyber operations.

From 2010 onwards, Ukrainian security researchers detected network intrusions and malware infections associated with Russian APTs, with codenames such as "Turla", "Red October", "The Dukes", and "NetTraveler" (Pernik, 2018, p. 61). Before 2014, these intrusions were generally geared towards espionage and focused on targets such as government organisations, the news media, political parties, and banks. However, the cyber campaign escalated significantly during the 2014 Ukrainian presidential election, in which Ukraine elected a successor to the recently deposed Yanukovych. This election was disrupted by a self-styled "Ukrainian hacktivist" group calling itself "CyberBerkut", which aimed to destabilise Ukraine's political system. A few minutes before the polls were scheduled to close, CyberBerkut vandalised the results website of the Ukrainian Central Election Commission, causing it to incorrectly display the far-right candidate Dmitry Yarosh as the winner (Koval, 2015, p. 56). This was an implausible fiction: in reality, Yarosh received a mere 0.7% of the vote, in contrast with the 54.7% share attained by the actual winner, the centrist candidate Petro Poroshenko. However, it dovetailed with Russian efforts to portray the Ukrainian government as captured by neo-Nazis; a narrative that would later be used as a pretext for a full-scale Russian invasion of Ukraine in 2022. After the election results website was hacked, a Russian state-run television station took a screenshot of the altered page and ran a news story declaring Yarosh to be the front-runner (Najibullah, 2014). It should be noted that there was no way for the hackers to change the underlying votes, which were recorded on paper ballots rather than electronically (Koval, 2015, pp. 56-57). As such, CyberBerkut's goal was not to "hack the election", but rather, to sow distrust in the integrity of the political process.

From 2015, Ukraine experienced a wave of cyber attacks against its critical infrastructure. Most of these were later attributed to the Russian APT Sandworm. In December 2015, hackers utilised the BlackEnergy malware platform to shut down a power plant in the west of Ukraine, blacking out the region's electricity grid for six hours during the middle of winter (Zetter, 2016). Although the blackout period was short, this was nevertheless a landmark incident in the history of cyber conflict. It was the second occasion, after Stuxnet, in which a cyber attack was used to cause destructive effects in the physical world. It was also the first occasion in which a power grid had been disabled

by computer hacking. It was also the first time that a physically destructive cyber attack had been directed against a civilian target (R. M. Lee, Assante, & Conway, 2016a, p. 20). Almost exactly one year later, Ukraine suffered a second cyber attack against its power grid, this time resulting in a one-hour blackout in Kyiv (Dragos, 2018, p. 11). The 2016 attack made use of a new and remarkably sophisticated malware platform, which was given the codename "Industroyer" by security researchers.[95] Like Stuxnet, Industroyer was specifically designed to infect industrial control systems. It was flexible and modularised, indicating that it was designed to be used against a variety of targets (Cherepanov, 2017, p. 2). The US security firm Dragos (2018, p. 11) suggested that the attackers could have inflicted significantly more damage if they had chosen to do so, and suggested that "the attack [may] have been more of a proof of concept than what was fully capable in the malware".

In 2017, Ukraine was hit by the massive NotPetya malware infection, which has also been attributed to Sandworm. This incident has been described as the costliest cyber attack of all time (Greenberg, 2019, p. 199). NotPetya was a self-replicating worm, designed to spread autonomously across networks and encrypt any computer it infected. It did not make use of any zero-day vulnerabilities; instead, it relied on a combination of two previously known exploits: Mimikatz, an open-source password-stealing tool, and EternalBlue, the stolen NSA exploit that was leaked by Shadow Brokers (Sood & Hurley, 2017). Using these two exploits in combination, NotPetya could gain a beachhead on a single unpatched computer and then spread to patched computers on the same network. Although it resembled criminal ransomware, it was designed solely for data destruction: there was no way to decrypt an infected device or even to pay the ransom (Ivanov, 2016). To start the infection, the attackers first breached the Ukrainian software company M.E.Doc, whose accounting software is used by almost every business in Ukraine (Cherepanov, 2017). The hackers then hijacked M.E.Doc's software updating process and used it to install NotPetya on its customers' computers.

After being initially seeded in this way, the malware began to spread autonomously across much of the Ukrainian internet. According to the Ukrainian government, NotPetya ultimately infected and disabled roughly 10% of all computers in the country (Associated Press, 2017). Additionally, NotPetya quickly spread to other countries, inflicting crippling damage on the Danish shipping company Maersk, the US pharmaceutical firm Merck, the Russian energy company Rosneft, and numerous other victims. The financial cost to Ukraine alone may have amounted to as much as 0.5% of that country's GDP (Pernik, 2018, p. 62), and the United States government estimated that

[95] This name was assigned by the Slovak security first ESET, which first discovered the malware platform. The malware is also coded as "CrashOverride" in some sources.

NotPetya caused US$10 billion in damage to the world economy, making it the costliest malware infection in history by a considerable margin (Greenberg, 2019, p. 199). Tom Bossert, the United States Homeland Security Advisor at the time of the incident, described NotPetya as "the [cyber] equivalent of using a nuclear bomb to achieve a small tactical victory" (quoted in Greenberg, 2019, p. 199).

The two power grid hacks and the NotPetya infection were the most highly publicised cyber attacks against Ukraine, but there were many others. Greenberg (2019, p. 47) observes that, in 2017, "practically every strata of Ukrainian society was being hit in successive waves of coordinated hacker sabotage: media, energy, transportation, finance, government, and military". In 2016, Ukrainian President Petro Poroshenko announced that his government had suffered 6,500 intrusions during the previous two months alone (Zinets, 2016). In December of that year, the Slovak security firm ESET reported that the Sandworm APT had carried out a wave of cyber operations against Ukrainian banks and financial institutions, which were geared toward data destruction rather than espionage (Cherepanov, 2016).[96] That same month, CrowdStrike reported that an Android application used by the Ukrainian military to target its field artillery had been hacked by Russia's military intelligence agency, the GRU (Meyers, 2016).[97] CyberX, a security firm, announced in 2017 that it had detected a large-scale cyber espionage operation against Ukraine's oil and gas infrastructure (Atch & Neray, 2017). That same year, a ransomware infection called "BadRabbit" briefly crippled the Kyiv metro system and Odessa airport, as well as Russia's central bank and two Russian media outlets (Leyden, 2017).

In 2018, Ukraine's domestic counterintelligence agency, the Security Service of Ukraine (SBU), announced that it had prevented an attempted cyber sabotage operation against a chlorine factory (Interfax-Ukraine, 2018). Soon after, the SBU announced that it had also thwarted an attempted cyber espionage operation against the country's judicial system (AP News, 2018). In 2019, the security firm Sentinel Labs identified a new espionage-focused APT that they codename "Gamaredon", which seemed to focus entirely on Ukrainian military, government, and national security-related networks (Kremez, 2020). Another security firm, QiAnXi, reported that an APT

[96] Sandworm is referred to as "TeleBots" in ESET's security reports.

[97] The CrowdStrike report was controversial: it initially claimed that the Android malware had allowed Russian-backed separatist forces in the Donbass to destroy 80% of Ukraine's D-30 howitzers; however, this claim was later retracted after it was disputed by Ukraine's Ministry of Defence. Nevertheless, CrowdStrike reiterated that the retraction did "not in any way impact the core premise of the report that the FANCY BEAR threat actor implanted malware into a D-30 targeting application developed by a Ukrainian military officer" (Dmitrova quoted in Kuzmenko & Cobus, 2017).

codenamed “Hades” (which seems to be one of the many aliases used by Fancy Bear) created a coronavirus-themed phishing email and used it to gain access to the Ukrainian Ministry of Health (Cimpanu, 2020). One of these emails – which falsely claimed that a Covid-19 infection had broken out in Ukraine – was forwarded outside of the Ministry and spread virally on social media, triggering violent riots across the country (C. Miller, 2020). Overall, there is probably no state that has ever been subjected to a more sustained or destructive cyber campaign than Ukraine in the period 2014 to 2022.

Can this cyber campaign be definitively attributed to Russia? The Russian government has consistently denied carrying out cyber operations against Ukraine or any other country (AFP, 2020). However, there is significant technical and contextual evidence linking the campaign against Ukraine with suspected Russian APTs. CyberBerkut, for example, is almost certainly a cover identity used by the Russian APT Fancy Bear, and not (as it claims) a domestic Ukrainian hacktivist group. A 2016 security report by Citizen Lab demonstrated that CyberBerkut had been responsible for leaking information that had previously been stolen by a Fancy Bear phishing operation, suggesting that these actors are part of the same underlying organisation (Hulcoop, Scott-Railton, Tanchak, Brooks, & Deibert, 2016, pp. 29-35). In 2018, an indictment by the US Special Counsel, Robert Mueller, identified Fancy Bear’s true identity as GRU Unit 26165 (DOJ, 2018a).

Most of the critical infrastructure attacks against Ukraine have been traced back to the suspected Russian APT known as Sandworm (Greenberg, 2019). A security report by ESET finds that NotPetya and Industroyer, the malware that was used in the 2016 power grid hack, were created by the same group of software developers (Cherepanov & Lipovsky, 2018). The ESET report does not link the malware developers to any particular government, but an internal CIA assessment that was leaked and reported by the *Washington Post* in 2018 concluded with “high confidence” that the NotPetya attack had been carried out by the Russian GRU (Nakashima, 2018). A month later, the governments of the United Kingdom, the United States, Canada, Australia, and New Zealand – the Five Eyes countries – all released public statements attributing the NotPetya attack to Russia (Muncaster, 2018). Of these, the British statement was the most detailed. It accused Russia of carrying out the NotPetya and BadRabbit attacks, as well as numerous other cyber operations against other states and international organisations. It also stated that CyberBerkut, Fancy Bear, and Sandworm are all aliases for the same underlying entity: the Russian GRU (NCSC, 2018). In 2020, a US indictment stated that Sandworm’s true identity was GRU Unit 74455 (DOJ, 2020). Collectively, the evidence suggests that a highly aggressive cyber campaign against Ukraine was primarily carried out by two

teams within the Russian GRU: Unit 26165 (Fancy Bear) and Unit 74455 (Sandworm). Both teams carried out hacking operations against Russia's adversaries; however, they seem to have adopted slightly different operational styles, with the former focusing on political disruption and the latter focusing on critical infrastructure hacks (Greenberg, 2019, pp. 243-270).

In light of the sustained cyber campaign that Russia conducted against Ukraine between 2014 and 2022, many observers anticipated that any escalation of hostilities between Russia and Ukraine would be accompanied by a major Russian cyber offensive. However, when Russia launched a full-scale Russian invasion of Ukraine in February 2022, the Russian cyber offensive largely failed to materialise. To date, the cyber component of the current phase of the conflict has been less prominent than many experts anticipated.

Certainly, there has been some use of cyber operations in the conflict. The CFR Cyber Operations Tracker, for example, lists 25 cases of significant Russian cyber operations against Ukraine during 2022 alone (CFR, 2022). The most notable Russian cyber operation took place on the day of the invasion. Viasat, a commercial provider of high-speed satellite broadband services, whose network is used by Ukraine as part of its command-and-control infrastructure, experienced a cyber attack that temporarily disabled one of its satellites (Nakashima, 2022). The Viasat network is used throughout Europe, and the operation caused widespread problems outside Ukraine's borders; the US government later publicly attributed the attack to Russia (Blinken, 2022). The Viasat incident is an example of the type of combined arms operation, mixing cyber and conventional capabilities, that many experts predicted would be commonplace for future wars. However, there do not appear to have been any significant follow-up cyber operations against Ukrainian infrastructure or its command-and-control systems. Most of the cyber operations carried out in the conflict have been unsophisticated and low-impact ones, such as DDoS operations and website defacements (Valeriano, Lonergan, W., & Jensen, 2022).

There are several possible explanations for this apparent puzzle. Some argue that the absence of major cyber attacks in the conflict demonstrates the fundamental weakness of cyber operations as an instrument of war, providing new evidence that the destructive capability of cyber conflict has been overhyped (Kostyuk & Gartzke, 2022; Valeriano *et al.*, 2022). By contrast, Rid (2022), suggests that cyber operations have played a significant role in the Russai-Ukraine war, but have been conducted in clandestine manner that is mostly concealed from the public view. Others speculate that Russia's cyber offensive was effectively countered by Ukraine's improved network defences, or

suggest that Russia's true cyber capabilities might be lower than analysts previously believed (Mallick, 2022, pp. 6-7). A complete historical accounting of the cyber component of the conflict will likely only be available in later years; perhaps after the war has concluded.

Until then, the most plausible explanation for the absence of visible cyber attacks is the intrinsic weakness of cyber operations as a method of coercion, as discussed in Chapter Three of this study. For Russia, cyber operations primarily function as a tool for signalling intentions to its adversaries and for undermining trust in technical systems. However, such signalling tools are predominantly useful before the outbreak of war. Once war begins, the time for signalling is over, and states must instead decide whether to act upon signals and threats they have issued previously. Once this threshold was reached, and Russia decided to use conventional weapons against Ukraine's civilian infrastructure, cyber attacks lost much of their relative utility. For example, if one wishes to destroy a power plant, it is much faster, easier, and more direct to launch a missile than to launch a cyber attack. Thus, once the conflict reached the stage where conventional options were available, Russia found it expedient to choose these options over cyber alternatives. If this interpretation of Russia's strategy is accurate, it implies that cyber conflict serves as a valuable "grey zone" tactic in conflict situations that exist between war and peace, but may be less effective in the context of a full-scale war.

6.2.3 Engaging in Great Power Rivalry

Russia has also used technical cyber operations to engage in rivalry with other great powers; in particular, the United States. As discussed in Chapter Five , the dyadic cyber conflict between Russia and the United States has tended to be less destructive and more restrained than either country's cyber operations against weaker states. Both states have resisted the temptation to attack the other using destructive malware platforms such as Stuxnet and Industroyer, presumably due to fears of escalation. Instead, cyber operations between the great powers have tended to focus on espionage, signalling, and positioning for the possibility of future conflict.

This pattern was evident in an early example of Russian cyber operations against the United States: the Agent.BTZ infection of 2008. According to a US government report, the operation was carried out by Russian intelligence officers in Afghanistan (NCCIC & FBI, 2016, p. 4). Some accounts of this event state Russian hackers left a malware-infected USB flash drive lying in a parking lot near a US military base in Afghanistan, and an American soldier picked it up and plugged it into one of the base's computers (Gostev, 2014). Whatever the truth of this account, the result was a massive

malware infestation that penetrated the Pentagon's non-classified and classified networks, spread across multiple countries, and took 14 months to fully remove (Shachtman, 2010). At the time, this event caused considerable nervousness in US defence circles; it was described as "the most significant breach of US military computers ever" by William Lynn III, the Under Secretary of Defence for Policy (Lynn III, 2010, p. 97). However, the underlying phenomenon – a state spying on another state's military – is a longstanding practice in international relations, and to some extent, an expected one.

Several subsequent Russian cyber espionage operations followed the same basic pattern of intruding into networks of high-profile political and military bureaucracies. In 2014, hackers successfully breached the non-classified network of the US State Department (Reuters, 2014). The hackers then used the State Department's email service to send spear phishing emails to Obama Administration staffers and thus were able to compromise the non-classified White House (Modderkolk, 2018). This allowed them to read President Barack Obama's non-classified emails, view his schedule, read some of his communications with US diplomats, and gain insight into internal discussions on US policy (Schmidt & Sanger, 2015). In August 2015, the same group of hackers carried out an intrusion into the Pentagon's non-classified email network, including the email system used by the Joint Chiefs of Staff (D. Martin, 2016; Reuters, 2015). Several months later, they carried out a spear phishing campaign to spy on US think tanks that deal with foreign policy issues (Adair, 2016; Reuters, 2015).[98]

These operations have been attributed to yet another suspected Russian APT: "Cozy Bear" (Nakashima, 2017a). Since Cozy Bear did not appear to coordinate directly with Fancy Bear, CrowdStrike suspected that this group was not part of the GRU, and was instead controlled by one of Russia's civilian intelligence agencies (Alperovitch, 2016). According to this analysis, Cozy Bear was probably controlled by either the SVR (Russia's externally focused civilian intelligence agency) or the FSB (its domestic counter-intelligence agency). These groups tend to compete with the GRU, rather than cooperate with it (Galeotti, 2016, pp. 3-4). CrowdStrike's suspicions were later confirmed by the Dutch newspaper *de Volkskrant*, which reported that the principal intelligence agency of the Netherlands, the General Intelligence and Security Service (AIVD), had hacked into the SVR's network (Modderkolk, 2018). From there, the AIVD was able to directly observe Russian hackers carrying out cyber operations against the United States, including its intrusions into the White House

[98] Among the think tanks and NGOs that were targeted in the latter operation were the Council on Foreign Relations, the International Institute for Strategic Studies, Eurasia Group, the Centre for a New American Security, and Transparency International (Adair, 2016).

and the State Department. The Dutch hackers even photographed the SVR agents who carried out the cyber operation, using security cameras in a nearby building to do so (Modderkolk, 2018).

In 2019 and 2020, the United States federal government suffered a massive cyber security breach across multiple agencies and organisations. This breach used a supply chain attack, similar to the hack of the Ukrainian software company M.E.Doc that was used to kickstart the NotPetya infection. In this case, hackers initially breached two technology services companies – SolarWinds and Microsoft – and then hijacked their software update mechanisms to install malware on computers used by their customers (Bing, 2020).[99] Thus, by successfully exploiting a small number of weak points, the hackers were able to gain access to a large number of organisations and computer networks. The SolarWinds supply chain attack allowed hackers to implant malware on 18,000 computers (Sanger, Perlroth, & Schmitt, 2021). Since SolarWinds software is widely used by the US government as well as private companies, this single operation probably allowed hackers to collect intelligence on numerous US government agencies, including the Departments of Commerce, Defence, Energy, Homeland Security, Justice, State and Treasury, and the National Institutes of Health (Wilson, 2020).

The SolarWinds supply chain hack was first discovered by FireEye (2020), which was itself one of the victims of the spying operation. Several US officials publicly blamed Russia for carrying out the operation, including Secretary of State Mike Pompeo and Attorney General William Barr (Sanger & Rappeport, 2021). Tom Bossert (2020) attributed the operation to Cozy Bear, saying that "[e]vidence in the SolarWinds attack points to the Russian intelligence agency known as the SVR, whose tradecraft is among the most advanced in the world."[100] On 5 January, four US government agencies issued a rare joint statement saying that the operation had been carried out by "an Advanced Persistent Threat (APT) actor, likely Russian in origin" (FBI, CISA, ODNI, & NSA, 2016).

6.2.4 Cyber Arms Control

As we have seen in the preceding sections, Russian technical cyber operations – especially those that have targeted states in its "near abroad" – have been exceptionally aggressive. However, there is

[99] Another software application, VMWare Workspace, was also exploited as part of the operation. This was an end-point software exploit, rather than a supply chain attack such as the ones carried out using SolarWinds and Microsoft services (Krebs, 2020).

[100] By contrast, President Donald Trump downplayed the likelihood of Russian involvement and speculated that the operation might have been carried out by China.

one element of Russia's technical cyber strategy that is unusual and, at first glance, seems to cut against the aggressive thrust of its overall strategy. This is the fact that Russia has repeatedly and consistently called for the creation of an arms control treaty that would place limits on state-sponsored cyber operations.

Russian diplomats have sought to realise such a treaty for more than two decades, in a long-running diplomatic campaign that is documented in depth by Chernenko (2018, p. 43) and Kurowska (2020, p. 87). Richard Clarke, the cyber security advisor to George W. Bush, describes Russia as "the leading advocate" of cyber arms control, and notes that the United States is "almost singlehandedly blocking" such an initiative (Clarke & Knake, 2010, p. 219). As early as 1998, Russian political leaders expressed fears over the "militarisation" of cyber space and inserted language on "information security" into a UN General Assembly resolution on internet governance (Chernenko, 2018, p. 44). At the time, Western efforts to promote international cooperation on cyber security, such as the 2001 Budapest Convention, were focused entirely on cyber crime and cross-border law enforcement issues. By contrast, Russia quickly realised that the internet could act as an arena for competition between sovereign states, and it sought to regulate such competition through a treaty analogous to the bilateral SALT and START agreements, or the multilateral Non-Proliferation Treaty.

In 2009, Vladislav P. Sherstyuk, the deputy secretary of the Russian Security Council (analogous to the National Security Council in the United States), gave a speech in which he outlined the provisions that a cyber arms control treaty might contain. He proposed banning the practice of implanting logic bombs in an adversary's network during peacetime; prohibiting cyber attacks against civilian infrastructure; and restricting anonymous cyber operations by governments (Markoff & Kramer, 2009). In 2011, Russian diplomats at the UN General Assembly (in conjunction with China, Tajikistan, and Uzbekistan) proposed a resolution calling for "an international code of conduct for information security". The proposed code contained very broad language, calling on member states "[n]ot to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies" (China, Russian Federation, Tajikistan, & Uzbekistan, 2011, p. 4). Since then, Russia has reiterated its desire to negotiate a treaty with the United States (Putin, 2020). It has also continued to propose cyber arms control within the United Nations, the SCO, and in bilateral negotiations with China, India, South Africa, Belarus, and Cuba (Chernenko, 2018, pp. 44-47).

This longstanding Russian desire to negotiate a cyber arms control treaty presents an interesting analytical puzzle. Russian diplomats have consistently argued that a treaty is necessary to prevent the "militarisation of cyber space", and yet Russia itself is one of the leading instigators of this militarisation. By some measures – for example, in its willingness to attack civilian critical infrastructure – Russia's technical cyber operations have been more aggressive than those of any other state. Russia clearly values its ability to disrupt and weaken its regional adversaries using technical cyber operations. Why then would Russian policymakers wish to establish an arms control treaty, which would require Russia to give up the cyber capabilities in which it has so heavily invested?

From a constructivist perspective, Russia's advocacy of cyber arms control could be seen as a form of non-rational status-seeking behaviour (Kurowska, 2020, p. 88). In this view, Russian foreign policy during the post-Cold War period can be understood as a struggle to achieve non-material goods such as prestige, respect, and recognition of its own "great power" status by the United States. From this perspective, a cyber arms control treaty, and arms control treaties more generally, would represent an end in itself. By sitting down to negotiate a treaty on a matter of great international importance, the United States would implicitly be treating Russia as a co-equal partner, as it did during the SALT negotiations during Cold War. The "status-seeking" explanation contains important psychological insights; however, it is inconsistent with the broader theoretical view of this study, which argues that state cyber strategies can generally be explained in terms of rational self-interest. Can Russia's seemingly contradictory policy on cyber arms control be explained in such rationalistic terms?

One simple way to solve the apparent contradiction is to assume that Russia is negotiating in bad faith. This is the view of Richard Clarke, who observes that when he was in government, he "viewed the Russian proposal as largely a propaganda tool" (Clarke & Knake, 2010, p. 219). This cynical view is not without justification. Several experts have argued that cyber arms control poses difficult – perhaps unsolvable – problems with verification (Borghard & Lonergan, 2018; Burgers & Robinson, 2018; Ford, 2010). Arms control treaties restricting nuclear reactors, long-range missiles, and conventional military forces are easier to verify, since these capabilities are difficult to conceal and can be detected through satellite surveillance. By contrast, a cyber "weapon" can be created by a small team of developers and stored electronically on a single flash drive. It can be reverse-engineered after it is used, which may offer clues as to the identity of its creators, but the attribution of any cyber operation is rarely certain. Thus, Russian policymakers may be willing to accept formal

limits on their cyber capabilities, secure in the knowledge that they would be able to circumvent those limits if they wished.

However, we do not need to impute such bad-faith motivations to explain Russian preferences for cyber arms control. If we assume that Russian support for cyber arms control is sincere and that Russia intends to give up its technical cyber capabilities after signing a treaty, this would result in an outcome that would be highly beneficial for Russian interests: a reduction in the cyber capabilities of the United States. As discussed in Chapter Five of this study, the technical sophistication of the cyber capabilities (for example, the malware associated with the Equation Group) exceeds that of all other states. While a hypothetical cyber arms treaty would deprive Russia of a useful foreign policy tool that it currently uses to promote its interests in its near abroad, it would still have many other levers available in this region, including economic statecraft, conventional military operations, and support for ethnic separatism. Meanwhile, the United States – a much more powerful adversary than Georgia, Estonia, or Ukraine – would be deprived of cyber capabilities that it might otherwise have used against Russia. For Russian strategists, this outcome would probably be seen as a net positive.

6.3 Russia's Use of Persuasive Cyber Power

The second major element of Russia's cyber strategy is its aggressive use of persuasive cyber power. This is the most distinctive and unusual feature of Russian cyber strategy. As previous chapters in this study demonstrate, both Brazil and the United States have adopted relatively restrained approaches to persuasive cyber power. There are some exceptions to this general pattern, such as attempts by the US State Department to advance American national interests through online public diplomacy or its support for censorship circumvention software. For the most part, however, these states have been reluctant to intervene too directly in the information markets and social networks of other states. Russia has no such qualms, and it has carried out several provocative cyber operations to undermine institutional trust in other countries. The following sections examine some notable examples of this aspect of Russian cyber strategy.

6.3.1 Amplifying Divisions in the United States

In 2012, the Russian government began to experiment with the use of "trolls" and "bots" to spread political messages on social media (Sanovich, 2018, p. 23). Unlike the various public diplomacy platforms used by the US State Department (see Chapter Five), these accounts operate covertly and do not identify themselves as representatives of the Russian state. At first, the Kremlin's social

media operations were primarily targeted at domestic audiences. Government-controlled social media accounts posed as ordinary Russians on websites such as VK and LiveJournal, wrote in the Russian language, and advanced simple propagandistic narratives in support of the Russian government (Sanovich, 2018, p. 27).

From 2014 onwards, Russia's persuasive cyber strategy seems to have undergone a shift. With the annexation of Crimea that year, Russia's relationship with the United States and European countries became increasingly adversarial. Western states responded with economic sanctions, which inflicted significant harm to the Russian economy (Åslund & Snegovaya, 2021, pp. 12-19). In this new political climate, the Russian government appears to have decided that persuasive cyber power could be used to advance its broader geopolitical strategy and began to direct its messages toward foreign publics. In 2014, *BuzzFeed News* published an investigative report that exposed the existence of the Internet Research Agency (IRA), an organisation in Saint Petersburg that serves as a hub for Russian persuasive cyber operations against other countries (Seddon, 2014). The IRA is ostensibly a private company, but it has no public-facing website, does not offer any services, and has no discernible business model. The organisation's financial backing comes from the Russian billionaire Yevgeny Prigozhin, a close political ally of Vladimir Putin and the owner of the Wagner Group, a private military company that effectively functions as an arm of the Russian state (DOJ, 2018b; Harding, 2019).

In 2014, the IRA created a team of English-speaking social media operators, who were instructed to pose as Americans on social media platforms and influence political discourse in the United States (Chen, 2015). Internal emails from within the IRA, which were leaked by Russian anti-government hacktivists, revealed that as of 2014 the organisation had an annual budget of US$10 million and employed roughly 600 people (Seddon, 2014). Those employees create and maintain thousands of fictitious personas on US-based social networks such as Facebook, Instagram, Twitter, and YouTube (Rosenberg, 2018). The working conditions at the IRA are demanding: employees are expected to "maintain six Facebook accounts publishing at least three posts a day and discussing the news in groups at least twice a day. By the end of the first month, they are expected to have won 500 subscribers and get at least five posts on each item a day. On Twitter, the bloggers are expected to manage 10 accounts with up to 2,000 followers and tweet 50 times a day" (Seddon, 2014).

At first, the IRA's English-language operations seem to have focused on advancing pro-Russian viewpoints on foreign policy issues – especially the Ukraine conflict. IRA-controlled accounts

attempted to seed the US information market with claims that the Euromaidan protests had been secretly organised by the CIA; that Ukrainian soldiers had committed atrocities against civilians in the Donbas region; and that the pro-Western government in Kyiv was composed of neo-Nazis (Soshnikov, 2017). Lyudmila Savchuk, a Russian journalist who went undercover and worked for the IRA for two months in 2015, said that her "central task" while working at the facility was "to spread negative publicity on Ukraine" (Savchuk, 2017). However, these operations do not appear to have been very effective. Despite the best efforts of the IRA, public opinion in Western countries remained both sympathetic to the Ukrainian position and supportive of economic sanctions against Russia – especially after a civilian airliner, Malaysia Airlines Flight 17, was shot down by Russian-backed separatists in Donbas (Pew, 2019). With this campaign, the IRA was effectively asking foreign audiences to trust the official position of the Russian government. The campaign failed because persuasive cyber power, as an offence-dominant technology, is not well suited to achieving this type of goal.

Russian strategists appear to have learned this lesson, and from roughly 2015 onwards the Russian cyber operations began to shift. Instead of trying to persuade Americans to trust Russia, the IRA's new approach focused on persuading Americans to distrust other Americans. The former objective was difficult to achieve, while the latter was made easier by the fact that the United States is riven with deep partisan divisions over issues such as race, immigration, police, and gun control. The IRA's preferred operational art was the use of "wedge tactics": it would identify partisan divisions in US politics and create different social media personas to argue both sides of the issue. By positioning IRA-controlled social media accounts on both sides of any given debate, the organisation sought to amplify extremist viewpoints and weaken the political centre of the United States. The ultimate goal of these efforts was to decrease the level of social cohesion and institutional trust within the United States, thereby reducing its ability to act assertively in international affairs.

Many of the most successful accounts used right-wing political messaging. The most successful account on Twitter during this period was @TEN_GOP, which claimed to be the "Unofficial Twitter of Tennessee Republicans" and amassed almost 150,000 followers. It was retweeted more than 6 million times between 2015 and 2017 (Cleary, 2019). Another account, @Pamela_Moore13, self-identified as "Southern. Conservative. Pro God. Anti Racism". It attracted 72,000 followers and was retweeted 2 million times. Other accounts controlled by the IRA adopted left-wing personas. These accounts typically focused on issues such as race relations, police violence, gun control, and the Black Lives Matter movement. Many of these left-wing accounts posed as African Americans and

addressed themselves primarily to black audiences. None of the left-wing Twitter accounts managed to reach the same level of following as @TEN_GOP, but many were nonetheless quite successful. Examples of IRA accounts in this category included @Crystal1Johnson ("It is our responsibility to promote the positive things that happen in our communities."), which attracted almost 57,000 followers and received more than 3.7 million retweets, and @TrayneshaCole, which cynically described itself in the following terms: "Love for all my people of Melanin. Your BLACK is BEAUTIFUL! #MyPussyMyChoice #BlackGirlsMagic #BlackLivesMatter". That account was retweeted on more than 585,000 occasions (Cleary, 2019).

The wedge issue that was used most frequently in Russian persuasive cyber operations during this period was the issue of race. In the aftermath of the 2016 US presidential election, a report by the US Senate Committee on Intelligence found that "race and related issues were the preferred target of the information warfare campaign designed to divide the country" (United States Senate, 2019, p. 6). The report goes on to note that:

> Evidence of the IRA's overwhelming operational emphasis on race is evident in the IRA's Facebook advertisement content (over 66 per cent contained a term related to race) and targeting (locational targeting was principally aimed at African-Americans in key metropolitan areas with), its Facebook pages (one of the IRA's top-performing pages, "Blacktivist," generated 11.2 million engagements with Facebook users), its Instagram content (five of the top 10 Instagram accounts were focused on African-American issues and audiences), its Twitter content (heavily focused on hot-button issues with racial undertones, such as the NFL kneeling protests), and its YouTube activity (96 per cent of the IRA's YouTube content was targeted at racial issues and police brutality). (United States Senate, 2019, pp. 6-7)

This tactic has been further documented by Stewart, Arif, and Starbird (2018), who constructed a network map of the discourse on Twitter surrounding the Black Lives Matter movement over nine months in 2016. The authors observed the presence of IRA-controlled accounts on both sides. These IRA-controlled accounts seeded extremist ideas within their respective clusters, which were then retweeted and spread through the network via a process of memetic transmission. The authors argue that the "presence of RU-IRA trolls in this conversation implies a calculated entry into domestic issues with the intent to polarize and destabilize [the United States]" (Stewart *et al.*, 2018, p. 4). Russian persuasive cyber operations also exploited a variety of other wedge issues to heighten

internal divisions within the United States. Many of these operations sought to exploit divisions over nationality, citizenship, religion, and regional identity. For example, an IRA-controlled Facebook page called "Being Patriotic", which had 4.4 million user interactions, tried to promote antipathy towards refugees, immigrants, and Muslims (McCarthy, 2017). The @TEN_GOP Twitter account was frequently used to promote Islamophobic conspiracy theories (Prokop, 2018).

The most extreme form of the IRA's wedge tactics, however, was its effort to promote the break-up of the United States. For example, Twitter accounts with left-wing personas were used to amplify calls for California to secede from the union (BBC, 2017). The idea of independence for California (which was branded on Twitter as "#Calexit") was raised in the aftermath of Donald Trump's presidential victory in 2016. Meanwhile, on Facebook, IRA-controlled pages such as "Heart of Texas" were used to support the idea of secession by Texas, or "#Texit" (DiResta *et al*., 2019, pp. 55, 70). At present, #Calexit and #Texit are both fringe political movements that are unlikely to lead to the dissolution of the United States. However, the Scottish and Catalan independence movements were also once considered part of the political fringe, and these movements have since become major players in the politics of the respective states. Russian support for regional secession in the United States can be seen as a form of "preparing the battlefield" – the persuasive cyber equivalent of installing a logic bomb on an adversary's server in advance of a possible future conflict. If political polarisation in the United States were to ever reach the point that regional secession became a realistic possibility, Russian persuasive cyber operations would likely be well-positioned to fan the flames.

In addition to these wedge tactics, IRA social media accounts made use of several other methods to advance Russian interests. Throughout 2016 and 2017, IRA-controlled social media accounts continued to promote Russian foreign preferences directly, in what amounts to a covert version of a traditional public diplomacy campaign. For example, the @TEN_GOP account, which was unusually vocal about foreign policy issues, tweeted criticism of NATO, criticism of US foreign policy in the Middle East, support for Marine Le Pen's candidacy in the 2017 French election and support for Bashar al-Assad's government in Syria (Prokop, 2018). Pro-Assad rhetoric, and criticism of US intervention in the Syrian civil war were consistent themes among IRA-controlled accounts on both the left and the right. IRA accounts with left-wing personas usually framed this position using anti-war and anti-imperialist rhetoric, while accounts with right-wing personas emphasised isolationist themes and promoted the idea that Assad could be a useful ally against ISIS (DiResta *et al.*, 2019, pp. 58-61). In terms of foreign policy, all IRA-controlled accounts, regardless of their self-proclaimed

ideological position, tended to promote a foreign policy of retrenchment: a mixture of "America First" rhetoric, distrust of foreign alliances, and withdrawal from institutional leadership.

Another common IRA tactic was the use of social media to create epistemic distrust in the United States. In this respect, the Kremlin's persuasive cyber operations abroad follow the same template that it uses in its domestic propaganda. Pomerantsev (2017, 2019), an astute observer of contemporary Russian society, argues that the style of this propaganda used by Vladimir Putin's government differs from more conventional forms of propaganda employed by totalitarian states in the twentieth century, including the Soviet Union. The Soviet Union remained rhetorically committed to the distinction between truth and falsehood: its public communications sought to convince its citizens that its positions were true and its enemies' positions were false. By contrast, Vladimir Putin's government has adopted a "postmodern" style of propaganda that seeks to promote an attitude of radical scepticism. A RAND Corporation study describes this style of propaganda as "the firehose of falsehood", arguing that it combines two salient features: "high numbers of channels" and "a shameless willingness to disseminate partial truths or outright fictions" (Paul & Matthews, 2016, p. 1). Russian citizens are subjected to a flood of obvious lies and conspiracy theories, which undermine trust in all epistemic authorities: the media, the government, civil society, intellectuals, opposition parties, foreign governments, and so on. Paradoxically, this ends up strengthening the government: in the absence of credible epistemic authorities to organise around, the political *status quo* remains unchallenged (Pomerantsev, 2014).

Since at least 2014, Russia has employed this postmodern style of propaganda in its persuasive cyber operations abroad. The result has been a series of operations that exhibit an almost surreal quality; almost as if they were a type of performance art. In one persuasive operation, outlined in detail by Chen (2015), the IRA staged an elaborate fake terrorist attack. Dozens of IRA-controlled Twitter accounts worked in concert to spread a false story that a chemical plant in Louisiana had been destroyed by ISIS. As part of the hoax, the IRA created doctored photographs of the explosion, set up fake news websites to report on the story, distributed a fake terrorist video on YouTube in which the Islamic State "claimed credit" for the attack, and even created a Wikipedia page to document the fake event. A few months later, the IRA used similar methods to create another elaborate hoax, claiming that there had been an outbreak of the Ebola virus in Atlanta, Georgia (Chen, 2015).

During the 2016 US presidential election, IRA-controlled accounts were used to promote a string of bizarre conspiracy theories, including the "Pizzagate" and "QAnon" theories, which claim that the US

government has been captured by a cabal of Satan-worshipping paedophiles (Hernandez, 2018). Russian government-controlled social media accounts have also been used to promote anti-vaccination views, with potentially dangerous public health consequences (Broniatowski *et al*., 2018, p. 1382). In 2019, Russian news outlets began promoting conspiracy theories about the negative health effects of 5G cellular networks; this later then morphed into the conspiracy theory that the Covid-19 pandemic had been caused by 5G signals (Temperton, 2020). Throughout 2020, the Russian state engaged in concerted operations to spread disinformation related to Covid-19, including theories that the pandemic had been deliberately created by Western elites to reduce the global population, claims that the virus had been manufactured to justify a transition to a socialist economic system, the promotion of unorthodox medical treatments, and spurious claims about the alleged dangers of Covid-19 vaccines (Matthews, Migacheva, & Brown, 2021, pp. 7-10).

Why has Russia used persuasive cyber power to promote these dangerous and destabilising conspiracy theories? How do these operations advance Russian interests? The fact that Russia has promoted both right-wing and left-wing points of view, as well as "anti-political" points of view, such as anti-vaccination sentiment, provides some insight into Russian strategic intentions. Most significantly, this suggests that Russian cyber operations are relatively unconcerned with altering US preferences, as Joseph Nye (1990, p. 168) suggests in his classic theory of soft power. Instead, Russia's goal seems to have been to reduce the stock of social cohesion and epistemic trust within the United States, thereby reducing the United States' capacity to carry out its foreign policy objectives. This is consistent with the neoclassical realist theories of Taliaferro (2006) and Schweller (2009), who point out that in order to pursue ambitious foreign policy goals, a state requires the ability to extract and mobilise resources from the society it governs. Conversely, a state that is internally divided and paralysed by epistemic distrust will be less capable of extracting and mobilising the resources necessary to support an assertive foreign policy.

6.3.2 Intervention in United States Presidential Politics

There is one Russian persuasive cyber campaign, in particular, that was so audacious and so consequential that it deserves special consideration. This was Russia's attempt to influence the 2016 US presidential election in support of the Republican candidate Donald Trump. This is a topic that became charged with partisan controversy in the United States between 2016 and 2019: it was the subject of a two-year investigation by special counsel Robert Mueller that was repeatedly described by President Trump as a "witch hunt" (Parker, 2017). Nevertheless, there is little reasonable doubt that the Russian cyber campaign did occur. The Mueller Report (2019), which constitutes the most

authoritative historical record of these events, provides detailed evidence of Russian attempts to influence the election. Furthermore, scholars such as Jamieson (2018) and investigative journalists such as Sanger (2018) independently confirmed and expanded on many of the details contained in the Mueller Report. A research paper by Almond, Du, and Vogel (2020, p. 3) has even demonstrated through quantitative analysis that pro-Trump trolling on Twitter fell by 35% on Russian holidays, and to a lesser extent, on days when there was cold weather in Saint Petersburg. The more interesting question is not whether the operation occurred, but *why* – what interests did Russia hope to achieve by involving itself in US presidential politics?

The Russian persuasive cyber campaign in support of Donald Trump had two major components. First, from February 2016 onwards, the IRA's network of social media accounts was directed to support Trump and to disparage the Democratic candidate, Hillary Clinton (Mueller, 2019, p. 23). According to a qualitative analysis by the consulting firm New Knowledge, which was commissioned by the United States Senate, IRA accounts with right-wing personas first supported Trump's candidacy during the 2016 Republican primary campaign, and were used to criticise Trump's Republican opponents (DiResta *et al.*, 2019, p. 80). During the presidential campaign, right-wing IRA accounts continued to support Trump and attack Clinton, while left-wing IRA accounts used a variety of tactics to reduce voter turnout. These accounts frequently attacked Hillary Clinton, drew equivalencies between her and Trump, and encouraged voters with left-wing views to boycott the election (DiResta *et al*., 2019, pp. 81-82). These accpimts also attempted to drive support for other left-leaning political figures, such as Senator Bernie Sanders, Clinton's opponent during the Democratic primary, and Jill Stein, the 2016 presidential candidate for the Green Party (Howard, Ganesh, Liotsiou, Kelly, & François, 2019, pp. 19, 34).

The IRA used a variety of operational tactics to deliver these messages to their intended audiences, including the use of paid advertising on Facebook, and organic posting on Facebook, Instagram, Twitter, and other social networks (Howard *et al*., 2019, p. 4). The IRA also used social media bots to drive up pro-Trump hashtags and manipulate content-sorting algorithms (Bessi & Ferrara, 2016). The IRA even used Facebook to organise dozens of pro-Trump political rallies across the United States, thereby blurring the line between the cyber domain and the physical domain (Mueller, 2019, pp. 29-31). These events would be organised by IRA accounts on Facebook and administered by unknowing Americans who were recruited to manage these events on the day.

The second component of the Russian cyber campaign was a series of targeted hacks against the Democratic National Committee (DNC) and the Clinton campaign. As early as 2015, the Dutch AIVD intelligence agency had penetrated the Russian SVR and observed Russian hackers carrying out operations against the Democratic Party of the United States (Modderkolk, 2018). The AIVD warned the US government about the intrusions, which in turn warned the DNC. However, a series of misunderstandings and miscommunications caused the DNC to underestimate the seriousness of the threat, and it waited seven months before hiring a cyber security firm to secure its network (Lipton, Sanger, & Shane, 2016). On 19 March 2016, the Russian APT Fancy Bear used a spear phishing operation to gain access to the personal Gmail account of Clinton's campaign chairman, John Podesta, and stole at least 50,000 emails from his archive (Franceschi-Bicchierai, 2016b; Mueller, 2019). The following month, Russian APTs used similar spear phishing tactics to gain access to the Democratic Congressional Campaign Committee (DCCC), the DNC, and the Clinton campaign (DOJ, 2018a). After a successful spear phishing operation against a DCCC employee, the Russian hackers implanted malware on the DCCC network and used it as a beachhead to gain access to the DNC mail server (Mueller, 2019, pp. 38-41).

All told, Russian hackers exfiltrated more than 70 gigabytes of data from the DNC server, in addition to emails already obtained from Podesta (Mueller, 2019, p. 40). After discovering the intrusions, the DNC retained the security firm CrowdStrike. CrowdStrike attributed these intrusions to the Russian APTs Fancy Bear and Cozy Bear, and linked these APTs in turn to the Russian GRU and SVR intelligence agencies (Alperovitch, 2016). Later, the Mueller Report attributed the hacking operations to two units in the GRU: Unit 26165 (Fancy Bear), and Unit 74455 (Sandworm) (Mueller, 2019, p. 36).

Instead of holding on to the intelligence it had gathered, the Kremlin released it to the public, in what appears to have been a deliberate attempt to damage Clinton's campaign. In June 2016, emails stolen from the Clinton campaign were released through DCLeaks, a website that claimed to be a WikiLeaks-style whistleblowing platform, but was actually controlled by the GRU (Mueller, 2019, p. 41). In the same month, the DNC and CrowdStrike announced that the DNC network had been compromised by two Russian APTs. Soon afterwards, a self-described Romanian hacker who called himself Guccifer 2.0 claimed that he had carried out the DNC hack on his own and began releasing emails stolen from the DNC as a form of proof (Koebler, 2016). However, in an online interview with *Vice News*, Guccifer 2.0's responses to Romanian questions in Romanian were poor and appeared to have been generated using Google Translate (Franceschi-Bicchierai, 2016a). Later, the Mueller

Report concluded that "Guccifer 2.0" was a fictitious persona created by the GRU, probably to reduce trust in the findings of cyber security researchers such as CrowdStrike (Mueller, 2019, p. 42).

The GRU then approached WikiLeaks, a whistleblowing platform run by the Australian activist Julian Assange, which had long been hostile towards Clinton (Mackey, 2016). Under the guise of the Guccifer 2.0 and DCLeaks personas, the GRU offered to send WikiLeaks the stolen emails for publication (Mueller, 2019, pp. 45-48). WikiLeaks accepted, and on 22 July, three days before the Democratic National Convention, it published 19,252 emails stolen from the DNC. The most damaging information in the leak was the revelation that, during the primary contest between Clinton and Bernie Sanders, the DNC had violated its formal role as a neutral referee and had instead shown favouritism towards Clinton (Blake, 2016). These leaks frustrated Clinton's attempt to unify her party after a divisive primary, and the hostility of Sanders' left-wing supporters continued to plague her campaign until the day of the election.

On 7 October, WikiLeaks released the email archive stolen from John Podesta. Once again, the timing of the release was bad for Clinton: the Podesta emails were released one hour after the *Washington Post* published the "Access Hollywood" video in which Trump appeared to admit to sexual assault. The release of the Podesta emails helped to distract from the Access Hollywood scandal and fed into several pre-existing negative narratives about Clinton: that she was too closely aligned with Wall Street elites; that her family's charitable foundation was corrupt; that her public positions were hypocritical and two-faced; that she supported a policy of "open borders" (BBC, 2016). These narratives continued to weigh Clinton down in the days leading up to the election. On 8 November, one month after the Podesta emails were released, Donald Trump won the presidential election.

To what extent did Russia's cyber operations influence the outcome? Is it possible that the Russian government was, in effect, able to select which candidate became President of the United States? In a strict sense, this question is impossible to answer: elections are complex and non-repeatable events, and it is extremely difficult to isolate the impact of any single causal variable. Nevertheless, this has not stopped a variety of observers from speculating. Clinton (2017, pp. 406-407) herself claims that if the Russian cyber operation had not taken place, she would likely have won. However, the respected pollster Nate Silver (2018b) points out that the resources that the Russian government deployed in support of Trump were relatively small compared to the resources that the Trump and Clinton campaigns were able to marshal in support of their respective candidates. He notes that the

IRA only had a monthly budget of around $1.25 million in 2016, which is dwarfed by the $1.2 billion that was spent by the Clinton campaign and its allied super PACs,[101] or the $617 million spent by the Trump campaign and its allied super PACs (Silver, 2018b). He also points out that, in quantitative terms, the IRA's content made up a tiny fraction of the enormous volume of election-related content that was posted on social media (Silver, 2018a). Based on this reasoning, he suggests that "if you wrote out a list of the most important factors in the 2016 election, I'm not sure that Russian social media memes would be among the top 100" (Silver, 2018c). Stanford researchers Way and Casey (2019, p. 2) similarly argue that "the weight of the evidence does not support the claim that Russia tipped the election in Trump's favor… Russian measures were drowned out by a range of domestic factors that supported Trump." By contrast, Jamieson (2018) provides a detailed argument that Russian interference was indeed decisive, and that in a counterfactual scenario in which the Russian cyber operation did not take place but all other variables were held constant, Donald Trump would not have won the presidency. If Jamieson is right, this would be an extraordinarily important and successful cyber operation – easily the most consequential use of persuasive cyber power by any state in the history of the internet.

During the 2020 US presidential campaign, in which Trump attempted to win a second term, many observers assumed that Russia would launch another cyber campaign to support him. However, the well-publicised successes of Russian persuasive cyber power during the 2016 election probably made it more difficult for that success to be repeated. In 2019, Fancy Bear hacked Burisma, a Ukrainian natural gas company that employed Joe Biden's son, Hunter Biden (Perlroth & Rosenberg, 2020). It was widely assumed that Russia's goal was to find damaging information about the Bidens that would increase Trump's likelihood of re-election; however, the Hunter Biden scandal failed to gain significant traction in the media, in part because news outlets were suspicious that the story might have emerged from Russia (Kessler, 2023).

Furthermore, several other states – seemingly inspired by Russia's example – also made attempts to influence the 2020 election. Graphika, a social media analysis firm, discovered a network of Chinese-controlled social media accounts attempting to promote anti-Trump YouTube videos (Nimmo, François, Eib, & Ronzaud, 2020, pp. 1-2). These videos were crude and propagandistic; the title of

[101] In the context of the political system of the United States, so-called super PACs ("political action committees") are non-profit organisations that engage in advocacy on behalf of political candidates. These organisations collect large amounts of money from donors and are allowed to engage in unlimited political spending in support of particular candidates. However, they are prohibited from coordinating their activities with the official campaigns of candidates they support (Vandewalker, 2013).

one of the videos, “When I voted for trump, I almost sentenced myself to death”, is indicative of the overall tone (Nimmo *et al*., 2020, p. 11). Meanwhile, Iranian hackers obtained the email addresses of American voters who were registered as Democrats (Bing & Stubbs, 2020). They sent political messages to those addresses posing as members of the Proud Boys, a far-right political group, and threatened voters with violence unless they changed their party affiliation to Republican (Corasaniti, Decker, & Saul, 2020). The Iranians who carried out the operation likely assumed that the notoriety surrounding the Proud Boys would drive media coverage of the story, thus amplifying the effect of the original emails. Their overall goal was probably to create the impression that the voter registration system itself had been hacked, thereby reducing confidence in the outcome of the election.

It seems unlikely that any of these persuasive cyber operations played a significant role in mobilising support for a particular party or candidate during the 2020 election. Nevertheless, all these persuasive cyber operations probably had the cumulative effect of undermining trust in US institutions. In the months before the 2020 presidential election, in response to these persuasive cyber campaigns, US Senator Marco Rubio (2020) argued that “[a]bove all, Russia and Iran want the losing side to reject the election outcome in order to undermine the winner’s legitimacy and spark a constitutional crisis”. This is precisely what happened: after Trump was defeated, roughly half of Republican voters concluded the election had been rigged (C. Kahn, 2020). On 6 January 2021, a group of far-right protestors stormed the US Capitol Building, seeking to overturn the election and calling for Vice President Mike Pence to be hanged. In the aftermath of that event, polling found that 45% of Republicans approved of the actions of the rioters (M. Smith, Ballard, & Sanders, 2021). After years of making use of persuasive cyber power to erode trust in US institutions, Russian officials might well have taken satisfaction from these results.

6.3.3 Dividing the European Union

In addition to its extensive operations against the United States, Russia has also engaged in a series of persuasive cyber operations against European countries. Way and Casey (2019, p. 3) find that between 2016 and 2019, Russia attempted to use persuasive cyber operations to influence the outcomes of elections or referenda in Bosnia, Macedonia, Montenegro, Italy, the Czech Republic, Spain, Germany, France, the Netherlands, and the United Kingdom. In all these cases, Russian was in support of candidates, parties, or referendum outcomes that would weaken international institutions such as NATO and the European Union.

One particularly notable cyber operation took place in the run-up to the 2017 French election, which sought to tilt the election in favour of the far-right candidate, Marine Le Pen. Before the election, Le Pen had promised that if elected, she would withdraw from NATO's integrated command structure and would hold a referendum on withdrawal from the European Union (AP News, 2017). The cyber operation in support of her candidacy became known as "#MacronLeaks", named after the Twitter hashtag that was used to amplify it. The most in-depth study of the #MacronLeaks cyber operation is Vilmer's (2019) report for the Atlantic Council, which argues that the operation consisted of three elements. The first of these was a disinformation campaign against her centrist opponent, Emmanuel Macron. This campaign started months before the election after it became clear that Macron would probably be Le Pen's main rival in the run-off. This disinformation campaign was spearheaded by Russian state media sources such as RT and Sputnik, which ran stories claiming that Macron was a "US agent" funded by a "very wealthy gay lobby"; these claims were amplified by American social media users linked to the "alt-right" ideological movement (Vilmer, 2019, pp. 4-9). The second element of the operation was a phishing attack on the cloud storage service used by Macron's campaign staff, which allowed the hackers to exfiltrate 15 gigabytes of confidential data (Auchard & Felix, 2017, p. 3; Vilmer, 2019). Finally, the files were released on social media approximately 44 hours before the election (Chhor, 2017).

Under French law, there is a 44-hour "blackout period" before an election, after which the media coverage of the election ends and the candidates are barred from making public statements. The timing of the leak seemed to be designed to coincide with the start of the blackout period, allowing news of the leaks to spread on social media while preventing the Macron campaign from issuing a public response (Chhor, 2017). Over the next two days, there was an organised campaign on social media to spread and amplify the leaks, which included the use of networks of bots to manipulate Twitter algorithms (Shaffer, 2017). The leaks did not contain any particularly damaging revelations, but the mere existence of a "Macron leak" created the impression of general malfeasance and wrongdoing. However, the campaign was ultimately unsuccessful: Macron defeated Le Pen by a decisive margin of 66% to 34%. In subsequent years, the #MacronLeaks case has mostly been studied as an illustration of the limits of persuasive cyber power (Vilmer, 2019). Coming late in the election cycle, and containing few specific revelations about Macron, the leaks were unable to overcome French voters' distaste for the far-right ideology of Le Pen.

France has never officially attributed responsibility for the #MacronLeaks incident (Uchill, 2017). However, there are two main suspects: the Russian state, and non-state alt-right groups based in the

United States. The original phishing attack against Macron's campaign bears similarities to the 2015 and 2016 cyber operations against the DNC in the United States, leading to widespread speculation that it was carried out by Russian intelligence agencies. Flashpoint, a US-based security firm, has investigated the operation and finds with "moderate confidence" that it was likely carried out by Fancy Bear (O'Neill, 2017b). Guillaume Poupard, the head of the French National Cybersecurity Agency (ANSSI), states that "[t]he modus operandi is very similar [to Fancy Bear]", although he warns that he "cannot exclude that a very competent group can try to imitate them" (quoted in Vilmer, 2019). Based on a careful analysis of the evidence available in the public domain, Vilmer (2019, p. 25) argues these two hypotheses should not be seen as mutually exclusive: both the Russian state and non-state alt-right actors share similar preferences, and there are strong reasons to believe they were both involved in spreading the leaks.

Russian-controlled social media accounts were also used to support secessionist movements in Catalonia and Scotland. In the aftermath of the 2014 referendum on Scottish independence (in which Scottish voters chose to remain part of the United Kingdom), pro-Kremlin social media accounts launched a coordinated effort to brand the referendum as rigged and called for a second vote (Nimmo, 2017). During Catalonia's attempted secession from Spain in 2017, Russian state media sources such as RT News and Sputnik generally adopted anti-Spanish and pro-secessionist stances and were among the most heavily-forwarded online sources in the Catalonian independence debate (Lesaca, 2017). Once again, these postings were amplified using a network of bot accounts, which helped to drive large volumes of social media traffic towards Russian state information sources. These two operations illustrate the use of Russian persuasive cyber power to increase division and conflict within the European Union; in this case, by supporting efforts to literally divide European states into smaller and weaker units.

Another case in which Russian persuasive cyber power may have been used in the context of European politics was the 2016 "Brexit" referendum in the United Kingdom. There is some evidence that Russia attempted to influence public opinion in the United Kingdom towards the Leave position, although the information available in the public domain is limited. A report by the British newspaper *The Times* analysed 156,252 Twitter accounts based in Russia and found that they had sent approximately 45,000 tweets about Brexit in the 48 hours before the poll (Mostrous, Bridge, & Gibbons, 2017). This is an interesting finding; however, this is a relatively low volume of social media posts, and it is difficult to imagine that it would have had a significant impact on the poll. Bastos and Mercea (2019, p. 51) identify a network of 13,493 Twitter bot accounts that participated in the

Brexit debate and were deactivated or shut down shortly after the referendum. Most of these accounts were used to support the Leave campaign; however, the authors of the study do not attribute the bot network to Russia or any other actor.

The Security Committee of the UK Parliament has published an official report on the question of Russian interference in the Brexit campaign. The report notes that the "preponderance of pro-Brexit or anti-EU stories on RT and Sputnik, and the use of 'bots' and 'trolls'" can be seen as "evidence of Russian attempts to influence the [EU referendum] process" in favour of Leave (Parliament, 2020, p. 12). However, the committee could not "establish whether there is secret intelligence which supported or built on these [open source] studies" due to the absence of cooperation from British intelligence agencies (Parliament, 2020, p. 12). In particular, the report notes that the committee requested information on the topic from MI5, the UK's principal counter-intelligence agency, and received only six lines of text in response (Parliament, 2020, p. 12). The unwillingness of the executive branch of the British government to investigate the issue contrasts sharply with the United States' thorough investigation of Russian persuasive cyber power during the 2016 presidential election, which produced two extraordinarily detailed reports by the United States Senate (2019) and Robert Mueller (2019). Overall, the evidence suggests that Russia did indeed use persuasive cyber power to support the Leave campaign. However, it is not known how widespread or effective this operation was, in part because of the United Kingdom's failure to adequately investigate the matter.

Finally, it should be noted that while the majority of cyber operations in this section involve Russia's use of persuasive cyber power in Western Europe, in recent years there has also been an increase in persuasive cyber operations in Eastern Europe and the Baltic states. A 2020 Mandiant report revealed the existence of a persuasive cyber operation designed to influence public opinion in Lithuania, Latvia, and Poland, which the firm dubbed "Ghostwriter" (Mandiant, 2020). The operation used a small network of falsified social media personas to advance a variety of anti-NATO and pro-Russian narratives, including the claim that NATO was responsible for spreading Covid-19 in Europe (Mandiant, 2020). The operation was small in scale, and Mandiant does not definitively attribute it to any state actor; however, it strongly implies that Russia was the culprit.

6.3.4 Insulating Russia's Information Market

This chapter demonstrates that the Russian state has, since 2012, systematically used persuasive cyber power to try to influence foreign audiences. At the same time, the Russian state has also

introduced a variety of "defensive" policies to insulate its population from being influenced by foreign actors.

On a technical level, the Russian government has engaged in steadily increasing censorship of its domestic internet. In 2012, the Duma passed an "internet blacklist" law that required all internet service providers to restrict access to a list of websites maintained by *Roskomnadzor*, the Russian government agency tasked with regulating public communications (BBC, 2012). The law was ostensibly passed to allow the government to block child abuse imagery, information about illegal drugs, and suicide techniques. However, the blacklist was quickly expanded to include websites that were seen as politically undesirable.

In the aftermath of the 2014 Russian occupation of Crimea, the blacklist was used to block the personal blogs of two notable members of the Russian opposition, Alexei Navalny and Garry Kasparov (Gutterman, 2014). In 2016, the *Roskomnadzor* banned the entire social network LinkedIn; access to the service was never restored (Reuters, 2017). In 2017, the French video-sharing website DailyMotion was banned (Mihov, 2017). In 2018, the Russian government attempted to ban the Telegram mobile messaging app, although Telegram is the most popular and successful online service that has emerged from within Russia itself. Russian internet users found technical methods to circumvent the ban and the app retained its popularity; after two years, the ban was rescinded (Reuters, 2020). In 2020, Russia attempted to ban several encrypted email services and VPN platforms that could potentially be used to circumvent bans on other websites (Bode, 2020). Finally, after Russia's 2022 invasion of Ukraine, the Russian government banned Facebook and Instagram, partially restricted access to Twitter, and banned Western government-funded news sites such as BBC News, Deutsche Welle, and Radio Free Europe (Al Jazeera, 2022; Bond & Allyn, 2022). As of 2022, Russia scores 23 out of 100 on the Freedom of the Net index, ranking it among the least-free countries in the world in terms of internet censorship (Freedom House, 2022).

Russia has also sought to use political and diplomatic tools to insulate its population against foreign ideas. At the 2014 NETmundial conference, for example, Russia was one of the leaders of the "digital sovereignty" coalition, which argued that internet governance should be shifted from the existing multistakeholder" model to a multilateral model in which the architecture of the internet would be governed by states through the ITU (Segal, 2016, pp. 218-221).[102]

[102] For more detailed discussion of the NETmundial conference, see Chapters Four of this study.

In accordance with its general preference for arms control (discussed in Section 6.2.4 of this chapter), Russia has engaged in repeated attempts at bilateral diplomacy with the United States aimed at reducing the use of persuasive cyber power by both states. In 2017, a report by *Buzzfeed News* revealed that Russia had secretly conducted exploratory negotiations with the Trump Administration to develop an agreement on mutual non-interference in each other's domestic politics (Hudson, 2017). The proposal ultimately fell through, in part because the United States was unwilling to give up its commitment to global internet freedom. According to one US official quoted in the story, "[w]e would have to give up democracy promotion in Russia, which we're not willing to do" (Hudson, 2017). In September 2020, during the final months of Donald Trump's presidency in the United States, Russia made another attempt to revive the idea of "arms control" in the persuasive cyber domain. President Vladimir Putin, perhaps considering the possibility that Joe Biden might defeat Donald Trump in the presidential election later that year, released a public statement calling for a "reboot" of US-Russia relations in the cyber domain. The statement lays out a proposal that includes four components, one of which would be the "exchange, in a mutually acceptable format, guarantees of non-intervention into internal affairs of each other, including into electoral processes, inter alia, by means of the ICTs and high-tech methods" (Putin, 2020). These proposals are intriguing, since they demonstrate the extent to which Russia views the United States' internet freedom agenda as a threat to its security.

6.4 Russia's Combined-Aggressive Strategy

This chapter demonstrates that Russia's strategy is highly aggressive in its use of both technical and persuasive cyber power. Russia employs cyber operations to disrupt weaker states within its region, as well as asymmetric tools to engage in great power rivalry with the United States. In peacetime, Russia uses technical cyber operations as a signalling mechanism, demonstrating its resolve and intention to escalate in areas where it feels its key interests are at stake. During wartime, it uses cyber operations as a force multiplier to enhance the effectiveness of conventional military operations – although the effectiveness of these wartime operations has been limited. Additionally, Russia actively utilises persuasive cyber-operations to disrupt social cohesion and erode institutional trust in other states. As such, the Russian case resembles the "combined-aggressive" ideal-type strategy outlined in Chapter Three of this study.

This strategy offers several clear benefits. Russia's willingness to use aggressive technical and persuasive cyber operations effectively gives it access to a wider range of foreign policy tools than it would otherwise possess. Russia's ability to hack critical infrastructure, cast doubt on election

legitimacy, increase political divisions, and decrease institutional trust in other states allows it to exert influence in numerous foreign policy contexts. American strategists often describe cyber operations as "grey zone" tactics, which fall into an ambiguous category between war and peace. Since Russia is weaker than its adversaries, with less power than either the United States or the European Union when the latter is treated as a collective, this ability to issue flexible responses to challenges, or escalate conflicts without resorting to all-out war, has proven attractive to Russian policymakers. Furthermore, the asymmetric nature of cyber conflict enables Russia to influence adversaries that are, according to traditional metrics, significantly more powerful. Persuasive cyber operations effectively serve as political *jujitsu*, using an adversary's strength against itself. Russia takes advantage of the online free speech that exists in Western political systems to undermine the institutions that Western states use to achieve their foreign policy goals.

		External Security Requirements	
		Low	High
Institutional Preferences	Positive	**"RESTRAINED STRATEGY"** Restrained use of technical cyber power Restrained use of persuasive cyber power	**"TECHNICAL-AGGRESSIVE STRATEGY"** Aggressive use of technical cyber power Restrained use of persuasive cyber power
	Negative	**"PERSUASIVE-AGGRESSIVE STRATEGY"** Restrained use of technical cyber power Aggressive use of persuasive cyber power	**"COMBINED-AGGRESSIVE STRATEGY"** Aggressive use of technical cyber power Aggressive use of persuasive cyber power **RUSSIA**

Figure 8: Russia's location within the typology of cyber strategies.

Yet, despite the apparent advantages of such a strategy, it is striking that no other state has been willing to fully adopt it. Certain states have adopted tactics that resemble Russia's cyber strategy in

particular areas – for example, the United States has been equally aggressive in its use of technical cyber power, and China has gone even further than Russia in its efforts to insulate its population from foreign persuasion. However, no other state in the world has combined Russia's use of state-sponsored computer hacking with its willingness to seed destabilising political narratives through social networks. The reason behind this is that Russia's strategy involves a set of costs and trade-offs that are particularly severe. By adopting this strategy, Russia has demonstrated an extraordinary willingness to take risks and accept strategic costs that other states would deem utterly unacceptable. The following sections will consider the various costs and trade-offs of Russia's cyber strategy.

6.4.1 Commercial Trade-offs

This study argues that states engaging in aggressive computer hacking, such as the United States, must be willing to accept certain trade-offs regarding their commercial and economic interests. Governments that hoard software vulnerabilities and conduct attacks on computer networks tend to undermine trust in technology companies originating from within their own country, and risk diminishing consumer trust in cyber security in general. It seems inevitable that this would act as a brake on their economic development.

The Russian example is instructive, as Russia has many of the fundamental ingredients necessary to build a vibrant high-technology sector, yet it has largely failed to do so in practice. Russia has a long tradition of excellence in computer science and mathematics dating back to the Soviet era. During the Cold War, Soviet leaders were fascinated by the concept of "cybernetics", which they viewed as the solution to the problem of information management in a centrally planned economy (Gerovitch, 2004). The Soviet Union made a serious effort to create a national internet before the United States, although the project ultimately failed due to political interference (Peters, 2016). Today, Russia has an excellent system of technical education that produces large cohorts of computer science graduates. During the 2008-2012 "interregnum" period, in which Dmitry Medvedev was the nominal president of Russia, he attempted to diversify the Russian economy and reduce its reliance on oil and gas by strengthening the technology sector (Malle, 2013). However, Russia has not been able to reduce its dependence on fossil fuels and continues to suffer from an immense brain drain problem, with many of its best graduates working for overseas firms rather than in the domestic Russian technology sector (Biagioli & Lépinay, 2019).

Some Russian technology companies, such as Yandex, primarily sell their services within the domestic Russian market. However, other Russian technology firms have expanded into international markets and these service-exporting firms have become collateral victims of the aggressive cyber strategies adopted by the Russian government. For example, the cyber security firm Kaspersky Lab, one of Russia's most successful technology companies, has been dogged by allegations that it is penetrated by Russian intelligence agencies. The governments of Germany and the United States, for instance, have issued warnings against using Kaspersky software (BBC, 2022). Much of the distrust toward Kaspersky is not motivated by specific security flaws in its software, but rather by a political assessment that "you can't operate in Russia without being controlled by the ruling party" (Firstbrook, quoted in Kramer & Perlroth, 2012). Another successful Russian technology start-up, the encrypted messaging app Telegram, was forced to relocate its operations to Dubai after repeated clashes with the Russian government due to the firm's unwillingness to hand over its encryption keys (Kravchenko, Al Ali, & Khrennikov, 2017).

Russia's broader failure to diversify its economy is not solely the result of its cyber strategy; on the contrary, the challenge of economic diversification has proven to be a thorny problem for most fossil fuel exporting states. However, the Russian government's insistence on treating its technology firms as tools of statecraft, and its apparent disregard for their business interests, have led to a significant trust deficit among consumers in foreign markets. This represents a genuine trade-off of Russia's cyber strategy.

6.4.2 Trade-Offs to Social Cohesion

A related problem is that Russia's aggressive use of persuasive cyber power tends to undermine institutional trust within Russia itself. This is the downside of the "firehose propaganda" system described by Pomerantsev (2019) and Paul and Matthews (2016). This model is fundamentally negative: it seeks to undermine trust in the foreign and domestic adversaries, rather than to foster a positive sense of trust in the Russian state and its institutions. Although this communication strategy has been successful in maintaining Vladimir Putin's domestic power, it has inadvertently contributed to the development of an exceptionally low-trust society, which in turn makes it more difficult for the Russian state's ability to mobilise societal resources toward collective goals.

One valuable source of comparative data on trust is the Trust Barometer maintained by Edelman, a public relations firm. This tool includes a Trust Index, a composite index of trust that measures total trust in NGOs, businesses, government, and the media across 27 countries. Individual states are

assigned a numerical score based on survey data. In this index, Russia has consistently ranked among the lowest-scoring countries. For example, in 2021, it received a score of 32, the lowest ranking of all the 27 states measured in the index. By contrast, the global average was 56, the United States scored 43, the Netherlands scored 57, and China scored 83 (Edelman, 2022, p. 21). There are multiple overlapping causes for these cross-national differences in trust: cultural attitudes toward authority, media norms, economic inequality, and variations in the quality of public administration all play a role. In the case of Russia, there is a long tradition of conspiracy theorising and distrust of authority dating back to the days of the Tsars; this is not a problem that can be solely attributed to Russia's cyber strategy. Nevertheless, it is striking that Russia, which routinely uses aggressive persuasive cyber power to erode trust among both foreign and domestic audiences, exhibits such low levels of institutional trust in comparative survey research. It seems unlikely that this is purely coincidental.

6.4.3 Balancing and Retaliation

A third trade-off of the Russian cyber strategy is the fact that it tends to provoke balancing behaviour and retaliation by other states. Estonia responded to the 2007 DDoS attacks by drawing closer to the NATO alliance and establishing a NATO Cooperative Cyber Defence Centre of Excellence in Tallinn (Gold, 2019). Ukraine responded to various Russian provocations between 2013 and 2022, including its destructive cyber operations, by drawing closer to the West and seeking membership in NATO.

This problem is evidenced by Russia's most famous persuasive cyber operation: its support for Donald Trump's 2016 presidential candidacy in the United States. In a narrow sense, this operation was a success. Russia's preferred candidate won the election, and the result is that the United States was paralysed by years of infighting between the White House and Democrats in Congress. As president, Trump made several moves that weakened the international position of the United States: he withdrew from the Trans-Pacific Partnership, cast doubt on US commitments to NATO, imposed tariffs on US allies, and reduced the United States' influence over international institutions. Since these results aligned with Russian national interests, Russian strategists might have been inclined to view this cyber operation as a stellar success.

However, the Trump presidency was not an unreserved success for Russia. Trump adopted many policies that were contrary to Russian interests: he imposed sanctions against Russia on 15 occasions between 2017 and 2019, withdrew from the 1987 Intermediate-range Nuclear Forces (INF) Treaty

despite vociferous Russian objections, launched a cruise missile attack against Russia's ally Syria, and initiated the US practice of supplying lethal military aid to Ukraine (Polyakova & Letsas, 2019). Furthermore, the United States imposed high costs on Russia in response to the cyber operation. Initially, these were not particularly severe: the Obama Administration expelled 35 Russian diplomats, shut down two estates that were used as holiday homes by Russian officials, imposed sanctions on the Russian GRU and FSB, and sanctioned three Russian companies that were accused of supporting the cyber operations (Sanger, 2016a). In 2017, however, the United States Congress followed this up by passing a sweeping new sanctions law, the Countering America's Adversaries Through Sanctions Act, which created far more significant costs for Russia. This piece of legislation imposed harsh sanctions on Russia and required the US government to sanction third-party states that purchase significant amounts of Russian arms or invest in Russia's oil and gas industry (Fried & O'Toole, 2019, pp. 5-6).

The most significant cost of the 2016 Russian cyber operation was not any specific US action or policy, but rather the general impression it created of Russia as an enemy of the United States, and the overall effect this had on subsequent relations between the two countries. Public opinion surveys demonstrate this trend starkly: in Pew's polling, in 2014 only 6% of Democrats and 5% of Republicans described Russia as the most dangerous enemy, but in 2017 this figure had risen to 39% of Democrats and 21% of Republicans (Pew, 2017). While Donald Trump hinted on several occasions that he would have preferred to follow a policy of *rapprochement* toward Russia, the atmosphere of anti-Russian distrust and suspicion that followed the 2016 election made such a policy impossible. Some analysts have even speculated that Trump might have felt "trapped" by his perceived relationship with Russia and that this might, paradoxically, have encouraged him to adopt more hawkish and anti-Russian policies than would otherwise have been the case (Polyakova, 2018). Perhaps, in a counterfactual world where Russia did not interfere in the election and Trump nevertheless became president, Russia would have been better positioned to take advantage of the situation and achieve some form of *rapprochement*. If such an opportunity ever existed, however, it was destroyed by the sense of bitterness that US elites felt in the aftermath of the Russian cyber operation.

Such dynamics provide a clear illustration of the pitfalls and trade-offs associated with the Russian cyber strategy, which helps to explain why other states have been hesitant to adopt a similar strategy. There are too many trade-offs: the economic costs, pervasive domestic distrust, and the possibility of international blowback created by this strategy are simply too high for other states to

accept. Why then has Russia adopted this strategy? The following sections will consider this theoretical puzzle.

6.5 Explanatory Variables

There have been several previous scholarly analyses that have tried to explain Russia's cyber strategy. Many accounts of Russian cyber strategy focus on Russia's strategic culture. These explanations point to the long-standing use of deception and internal destabilisation by Russian governments during the communist and even Tsarist eras, as well as the modern Russian doctrines of "hybrid" or "non-linear" warfare. For example, Rid (2020) regards Russian cyber operations as essentially a continuation of the policy of "active measures" by the Soviet Union to destabilise the capitalist world. Klimburg (2017) similarly looks back to the Soviet era, when the USSR emphasised the importance of cybernetics as a tool for realising the benefits of communism. Kello (2017, p. 220) argues that "the essence of Russia's modern information warfare doctrine… is the belief – Bolshevik in its historical origins, civilisational in its political implication – that modern conflict centres on domination of information rather than geographic space". Other authors point to more recent developments in Russian strategic thinking. A study by the RAND Corporation on Russian foreign policy, for example, describes Russian strategic culture as having a preference for "grey zone" tactics that blur the lines between war and peace (Pettyjohn & Wasser, 2019). Lilly and Cheravitch (2017) similarly argue that Russia's cyber strategy is driven by the institutional culture of Russia's military and intelligence agencies, including their perceptions and their military doctrine.

Greenburg's (2019) history of the Sandworm APT similarly argues that Russia's cyber operations are an expression of its broader strategic culture, epitomised in the so-called "Gerasimov Doctrine". The concept of the Gerasimov Doctrine draws its name from a 2013 article by the Russian Chief of the General Staff, Valery Gerasimov, which was later translated and published online by Mark Galeotti. In the article, Gerasimov makes the following observations:

> The very "rules of war" have changed. The role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness. […]
>
> Asymmetrical actions have come into widespread use, enabling the nullification of an enemy's advantages in armed conflict. Among such actions are the use of special-operations forces and internal opposition to create a permanently operating front

> through the entire territory of the enemy state, as well as informational actions, devices, and means that are constantly being perfected. […]
>
> The information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy. In North Africa, we witnessed the use of technologies for influencing state structures and the population with the help of information networks. It is necessary to perfect activities in the information space, including the defence of our own objects. (Gerasimov, quoted in Galeotti, 2014)

It should be noted that the Gerasimov Doctrine is not a formal military doctrine, and this term is not used in official Russian government sources. Moreover, these passages describe Russia's perception of *Western* actions in Libya, rather than a description of Russia's strategic plans. For these reasons, Galeotti (2014), the scholar who coined the phrase "Gerasimov Doctrine", has since attempted to retire the term. Nevertheless, the terminology has stuck, in part because Gerasimov's words seem to anticipate Russia's future cyber operations with eerie prescience, and because his remarks offer insight into the strategic culture that birthed these operations.

A third family of explanations tries to explain Russia's cyber strategy as being the product of Russia's domestic institutions. For example, Klimburg (2017) argues that Russia's choice of cyber strategy has been influenced by the makeup of Vladimir Putin's domestic coalition, including the prominent role played by former members of the security community (the so-called "*siloviki*") and the Russian government's connections to organised crime. These actors are familiar with unconventional tools such as covert operations, political subversion, and cyber crime, and tend to incorporate similar tactics into their foreign policy toolkits. Galeotti (2016, 2021) focuses on the organisational structure of the Russian intelligence and security community, with what he describes as a "multi-headed hydra" or an "adhocracy": a sprawling collection of agencies, each with their own agenda, operating in a relatively uncoordinated fashion, which in turn gives Russian cyber operations a seemingly chaotic and unpredictable character.

A fourth family of explanations focuses on the personality of the individual leader as the preferred level of analysis. These explanations tend to focus on Vladimir Putin's psychology and personal history, including his career as an intelligence officer, his high level of risk tolerance, his adversarial relationships with other world leaders, and his zero-sum views on international relations. For example, Marten (2015) characterises Putin as an improvisational risk-taker who is motivated by his

individual political interests and his desire to signal strength to domestic audiences and argues that these factors offer the most compelling explanation for Russian foreign policymaking. Galeotti (2019) holds a similar view, describing Putin as an improvisational risk-taker rather than a careful strategist. Interestingly, former US Secretary of State and presidential candidate Hillary Clinton (2017) adopts a similar mode of explanation in her memoir, arguing that Russia's cyber operations during the 2016 US presidential election were motivated, in part, by personal animosity between herself and Putin.

Finally, some scholarship argues that Russia's cyber strategy is motivated by an ideological hostility toward democracy and liberalism. McFaul (2020, p. 111), for example, argues that Putin is motivated by his sincere belief in "illiberal conservativism", an ideological worldview that is grounded in Orthodox Christianity and is hostile towards Western-style social liberalism. McFaul (2020, pp. 137-138) argues that Russian interference in the 2016 US presidential election, for example, did not significantly advance Russian national interests and cannot be explained from a realist perspective. Instead, he argues that the operation can only be explained if we assume that "Putin sought [in Donald Trump] an ideological soulmate for promoting nationalist, conservative ideas, similar to his friends, Orbán, Le Pen, and Farage" (McFaul, 2020, pp. 137-138). This ideology-centred explanation for Russian cyber strategy is fairly common in the popular media. For example, historian Anne Applebaum (2022), in an essay in *The Atlantic*, argues that Putin regards himself as being in an ideological conflict in which he is "fighting the world's democracies". This interpretation has also been advanced by US government officials, including former CIA Director David Petraeus (cited in Gvosdev, 2019, p. 323). For the most part, scholars in the field of International Relations have tended to be more sceptical of these ideological explanations for Russian foreign policy. Since many aspects of Russia's foreign policy have remained consistent across different regime types and ideological periods, national interest appears to be a more useful variable than ideology for explaining it.

Indeed, a simpler explanation for Russia's cyber strategy is that it aligns with the country's national interests. According to Gvosdev (2019, p. 321), Russian cyber strategy should be understood in realist terms, as a set of actions designed to advance Russian strategic interests. Jensen, Valeriano, and Maness (2019) argue that cyber conflict is a low-cost, low-risk tool Russia employs to compel, deter, and disrupt the United States. From this perspective, Russia's choice of strategy is not a theoretical puzzle that requires explanation; instead, it simply reflects the self-evident fact that "[g]reat powers use any means at their disposal to advance their interests" (Jensen *et al*., 2019, p.

213). However, these explanations are clearly incomplete. Other states such as Brazil and the United States also possess the means to conduct aggressive persuasive cyber operations, but there are significant differences between their cyber strategies and that of Russia. To provide a satisfying realist explanation for Russia's cyber strategy, we must account for this variation – we need to understand what sets Russia's interests apart. The following sections will argue that two independent variables offer a useful and parsimonious explanation for Russia's distinctive cyber strategy: its external security requirements and its institutional preferences.

6.5.1 External Security Pressures

Russian foreign policy has traditionally been shaped by the high external security requirements of the Russian state (Graham, 2010, p. 55; Kotkin, 2016, p. 4; Larrabee, 2010; Mearsheimer, 2014). This motivation has been present in every period of Russian history, including the imperial period, the communist period, and the post-communist period. In the imperial period, Russian leaders were motivated primarily by the "survival of the empire and the maintenance of its territorial integrity" (Hosking, 1997, p. 41). Soviet foreign policy during the Cold War was grounded in a "traditional and instinctive Russian sense of insecurity", according to US diplomat George Kennan (1946, p. 5). A consensus report by a large group of US experts on Russian foreign policy argues that, during the post-Cold War period, Russia has been motivated by "a deep-seated sense of geopolitical insecurity which motivates it to pursue strategic objectives that establish an uncontested sphere of influence in the post-Soviet region" (DOD, 2019).

It is possible to draw a clear line from Russia's high external security requirements to its adoption of an aggressive cyber strategy. As is the case with the United States, Russia faces the problem of disjuncture between its ends and means. Russia wishes to protest its vast geographic borders; maintain a sphere of influence within it near abroad; destabilise governments in neighbouring states that it considers hostile; expand its influence in other regions such as the Middle East and Africa; and challenge the global dominance of the United States. Most importantly, Russian foreign policy during the post-Cold War era has sought to prevent hostile concentrations of power from forming along its borders, which has had the effect of bringing Russia into conflict with NATO and the EU. However, Russia lacks the conventional economic and military tools to achieve these expansive goals. As a result, Russia has supplemented its conventional military strength with a variety of non-military foreign policy tools, including covert operations, soft power, economic statecraft, and cyber conflict.

Russia's high external security requirements are, in part, the result of its natural and political geography. Russia's fundamental geopolitical challenge is that it has poorly defensible borders with few natural mountain ranges or bodies of water to act as barriers against potential aggressors (Friedman, 2008). The consequence of this is that Russia has suffered at least one major invasion in every century throughout its modern existence: it was invaded by the Crimean Tatars in 1571; Poland-Lithuania in 1605; the Swedish Empire in 1708; the French Empire in 1812; Germany in 1915; and Germany once again in 1941. To overcome this weakness, Russia's rulers have repeatedly sought strategic depth, pushing their borders outward to increase the distance that an invading army must cross before it can reach Moscow or Saint Petersburg. This policy of expansion reached its apex after the aftermath of World War II, when Josef Stalin controlled a Soviet empire whose border effectively reached the centre of Germany. However, Russia's post-World War II expansionism proved to be unsustainable. Eastern Europe repeatedly rebelled against Russian rule, forcing the Soviet Union to put down uprisings in Hungary in 1956 and Czechoslovakia in 1968. When Poland rebelled in the 1980s, the Soviet Union was no longer powerful to repress it and the system rapidly unravelled, causing Russia to lose control over Eastern Europe, the Baltic states, Belarus, and Ukraine. More than two centuries of Russian territorial gains were lost in the period from 1989 to 1991, with the newly formed Russian Federation retreating to the approximate borders the Russian Empire had occupied before the reign of Catherine the Great (1762-1796).

In the immediate post-Cold War era, during the tenure of Foreign Minister Andrei Kozyrev, Russia tried to develop a more cooperative relationship with Western Europe and the United States. However, this policy of accommodation was soon abandoned, and Russia quickly reverted to its traditional foreign policy goal of establishing a sphere of influence in the former Soviet republics (Page, 1994, p. 812). There is some debate as to why a lasting accommodation between Russia and the West was not achieved. Some sources suggest that Russian exceptionalism caused its leaders to adopt an overly broad conception of Russian interests, essentially causing them to view the newly independent states of Eastern Europe and Central Asia in quasi-imperial terms (Bykova, 2022). Other scholars argue that the United States behaved in bad faith, promising that it would refrain from expanding NATO into Russia's near abroad and then going back on these commitments when it seemed that Russia was too weak to object (Shifrinson, 2016; Ziegler, 2021).[103] Regardless of who is

[103] Authors that are critical of the role of the United States in the conflict are quick to point out that "sphere of influence" politics is not an exclusively Russian phenomenon, and that all great powers try to surround themselves with friendly client states. For example, Jervis (1978, p. 169) observes that all "seek to control, or at least to neutralize, areas on their borders", while Mearsheimer (2003, p. 141) argues that the primary goal of all great powers is "to dominate their own region". The United States has been very protective of its own

to blame, the fact remains that Russia regards itself as having expansive political interests within its region. By the late 1990s, Russia had come to regard Western states as a threat to those interests.

Several events marked this shift toward conflict. In 1999, NATO was expanded to include the Czech Republic, Hungary, and Poland. In the same year, NATO carried out a military intervention against Serbia, a longstanding ally of Russia, resulting in its secession of Kosovo. Under the administration of George W. Bush, the United States sought to develop strategic defences against nuclear missiles, which Russia regarded as a direct threat to its deterrent capability. The United States invaded Iraq despite Russian objections, deployed NATO forces to Afghanistan, and in 2004 enlarged NATO to include the former Soviet republics of Latvia, Lithuania, and Estonia. In the early 2000s, there were a series of "colour revolutions" against pro-Russian governments along Russia's borders – most notably the 2003 Rose Revolution in Georgia, and the 2004 Orange Revolution in Ukraine. Russian policymakers regarded these events as foreign-sponsored coups, rather than genuine expressions of democratic sentiment, and feared that the Russian government itself might be susceptible to a similar uprising. All these developments contributed to a genuine fear among Russian policymakers that they were being encircled. At the Munich Security Conference in 2007, Vladimir Putin stated that the United States' foreign policy had created a deep sense of insecurity within Russia:

> One state and, of course, first and foremost the United States, has overstepped its national borders in every way. […] And of course, this is extremely dangerous. It results in the fact that no one feels safe. I want to emphasise this – no one feels safe! (Putin, 2007)

When the Obama Administration took office in 2009, the relationship between Russia and the West had become highly antagonistic. Although Obama hoped for a "reset" of relations between the two countries, the United States continued to take actions that Russia perceived as hostile: it supported Syrian rebels during the Syrian civil war, participated in the 2011 NATO intervention in Libya that resulted in the overthrow of Muammar Gaddafi, and most importantly, it supported the overthrow of the pro-Russian government of Victor Yanukovych in Ukraine in 2014. Although this latter event was driven by domestic Ukrainian opposition to Yanukovych's policies, Russia regarded it as an American covert operation designed to remove one of the "buffer states" along its borders. In his

---

sphere of influence in the Americas. For example, it entered World War I in part to prevent a German alliance with Mexico (Tuchman, 1985, pp. 170-171); during the Cold War, it felt deeply threatened by the Soviet Union's alliance with Cuba (Bain, 2006, p. 145).

speech announcing the Russian annexation of Crimea, Putin claimed that the United States was engaged in a concerted effort to encircle and contain Russia:

> We have every reason to assume that the infamous policy of containment, led in the eighteenth, nineteenth, twentieth centuries, continues today. They are constantly trying to sweep us into a corner because we have an independent position, because we maintain it and because we call things like they are and do not engage in hypocrisy. (Putin, 2014)

To overcome this perceived insecurity, Russia spends an unusually large percentage of its GDP on defence. Between 2005 and 2022, defence spending consumed 3.86% of Russia's GDP, compared to a global average of 1.93% (SIPRI, 2022).[104] However, the Russian economy is only about one-tenth the size of the European Union's economy and one-fourteenth the size of the US economy. Although Russia maintains high levels of military spending and has large quantities of military equipment that it inherited from the Soviet Union, the limited size of Russia's economy means it is unable to compete with Western states in terms of absolute military expenditure. As a result, Russia lacks the conventional military and economic capability to achieve all its ambitious foreign policy goals. The limits of Russian military power in the post-Cold War era have been starkly demonstrated by Russia's failed invasion of Chechnya in 1994, the explosion of the submarine *Kursk* in 2001, and the enormous difficulties that Russia experienced in its 2022 invasion of Ukraine (Golts, 2023).

To overcome these weaknesses, Russia has developed a variety of non-military foreign policy tools and force-multipliers. These tools include its veto power on the UN Security Council, which it inherited from the Soviet Union; a large nuclear arsenal that is used for coercive diplomacy; its ethnic and cultural ties with Russian-speaking minorities in post-Soviet states; its gas and oil pipelines to Europe; its broadcast media networks such as RT and Sputnik; and military auxiliaries and irregulars (such as the "little green men" that were used to seize Crimea in 2014). Collectively, these tools are sometimes described as "grey zone" capabilities, as they seem to occupy a position between peace and war (Pettyjohn & Wasser, 2019). This force-multiplying toolkit also includes technical and persuasive cyber operations. Through the use of these instruments, Russia has been

[104] Previous chapters of this study point out that defence spending is a good indicator of the level of importance that a state attaches to security issues. United States, which also has high security requirements due to its ambitious and expansive foreign policy goals, has a correspondingly high level of military expenditure. By contrast, Brazil, which has low external security requirements due to its more limited foreign policy goals and its secure geographic position, has low military expenditure.

able to signal its intentions to impose costs on neighbouring states that align with the West and destabilise neighbouring states that it considers hostile. It has also managed to significantly amplify internal political divisions within the United States, disrupting United States' ability to conduct a unified and assertive foreign policy. Without Russia's aggressive cyber strategy, it would have been more difficult for Russian policymakers to pursue these ambitious goals simultaneously.

These actions seem to be driven by a consistent underlying strategic logic. From Moscow's perspective, Russia has a core interest in maintaining political influence in its near abroad, in order to prevent another major power from using one of its neighbours as a staging area for an attack. As such, Russia seeks to discourage its neighbours from aligning with other great powers or military alliances. This objective is accorded such importance that Russian policymakers are willing to employ military force to achieve it, as demonstrated during the 2008 war against Georgia, the 2014 invasion of Crimea and the Donbas, and the 2022 full-scale invasion of Ukraine. However, cyber operations serve as a useful "intermediate" tool in situations where Russia wishes to pursue this foreign policy objective without incurring the costs of war. By obscuring attribution, Russian cyber operations generate enough plausible deniability to minimise the risk of repercussions. Nevertheless, the message sent to Russia's adversaries is unambiguous: they cannot entirely trust their technological systems, and crossing Russia's red lines will result in negative consequences.

However, cyber conflict is not a magic bullet. Many of Russia's cyber operations have failed to achieve their goals. For example, Russia's cyber operations against the Baltic states have not dissuaded these countries from aligning themselves with NATO; on the contrary, states such as Estonia have instead aligned more closely with NATO since 2008. However, these failures should not lead us to conclude that Russia's cyber strategy is irrational. On the contrary, many of these failures simply reflect the difficulty of achieving Russia's strategic goals. In any reasonable counterfactual scenario, it seems likely that nearby post-communist countries such as the Baltic states would have tried to align themselves with the West. For these states, Russia's geographical proximity and its history of seeking regional hegemony present an obvious security threat. Therefore, it is logical that Russia's neighbours would seek to increase their level of security by aligning themselves with powerful offshore balancers such as the United States. In other words, Russia's failure to achieve its foreign policy goals reflects, in part, the difficulty of the goals it aspires to, rather than the weaknesses of the strategy it uses to achieve them.

Overall, Russian foreign policymakers, having set out to achieve a difficult set of goals, and with relatively few tools at their disposal, have made use of several risky and unconventional tactics to achieve these goals. This has led directly to the growth of Russia's cyber capabilities and the adoption of its aggressive cyber strategy.

6.5.2 Institutional Preferences

Russia's "combined-aggressive" cyber strategy cannot be explained solely by its external security requirements. As discussed in Chapter Five, the United States also has high security requirements stemming from its expansive and ambitious foreign policy interests. However, while the United States has responded to these security pressures by aggressively employing technical cyber power, it has not used persuasive cyber power in the same subversive manner as Russia. This is the most anomalous aspect of Russian cyber operations, and any theoretical explanation of Russia's cyber strategy needs to account for it.

Why is Russia so distinct in its use of persuasive cyber power, even compared to other countries that also face high external security pressures? To answer this question, we need to consider a second variable: Russia's institutional preferences. With one notable exception, Russia's institutional preferences are "negative". Instead of creating or strengthening institutions to advance its interests, Russia focuses on weakening international institutions it perceives as constraining or hostile. Since persuasive cyber power is an offence-dominant tool, it is particularly well suited for realising these preferences, providing Russia with a strong incentive to utilise it more intensively.

Russian foreign policy is heavily influenced by its active opposition to the two most important institutions in its immediate geopolitical region: the European Union and NATO. Russia is particularly hostile toward NATO, which was founded in 1949 as a collective security agreement to help Western states balance against the Soviet Union. Following the Cold War, there was a brief period of accommodation between NATO and the Russian Federation. Russia was invited to join NATO's Partnership for Peace programme in 1994, and a permanent NATO-Russia Council was created in 2002 to facilitate cooperation between the two sides. There is some evidence that Vladimir Putin hoped Russia could join NATO during the early stages of his presidency; although, one suspects that Putin would have tried to sabotage the alliance from within (Roache, 2019). In any event, NATO's bombing of Serbia in 1999, "out of area" operations in Central Asia and Africa, and expansion to include former Warsaw Pact and Soviet Union members eliminated any possibility of lasting accommodation, leaving Russia feeling increasingly isolated and threatened.

These developments led Russia to view NATO as an anti-Russian alliance and to adopt a strong preference for weakening NATO and preventing its further expansion. To realise this preference, Russia has carried out persuasive cyber operations in support of political candidates and movements within Western states that express scepticism towards NATO. It is in this context that Russia's extraordinary intervention in the 2016 US presidential election should be understood. The emergence of Donald Trump during the 2016 Republican primary created an unusual situation in which a NATO-sceptical politician had the potential to become the candidate for one of the United States' two major political parties. When this rare opportunity presented itself, the Russian government seized it wholeheartedly and went to extreme lengths to support Trump's candidacy. This is very similar to the #MacronLeaks operation prior to the 2017 French election, in which Russia appears to have supported the NATO-sceptical candidate Marine Le Pen. Russian hostility toward NATO provides a satisfying and consistent explanation for these persuasive cyber operations, in contrast to explanations that emphasise Vladimir Putin's ideology or his supposed personal affinity for the Western politicians that Russia supports.

Although Russian official rhetoric toward the European Union is somewhat less hostile than its views on NATO, Russian institutional preferences regarding the EU are similarly negative. European solidarity has been weakened by events such as the post-2009 Eurozone debt crisis, the 2015 Syrian migrant crisis, and the Brexit referendum. Despite these problems, there are good reasons for Russia to feel threatened by the EU. While the prospect of a federal Europe now seems much less likely than it did during the 1990s, there are powerful ongoing incentives for cooperation and integration within Europe, including cooperation in the security sphere. As recently as 2018, French President Emmanuel Macron attempted to revive the idea of a "European army" (BBC, 2018). A European Union that possessed a common foreign policy and an integrated military command would be a first-rate world power, regardless of whether it adopted a formal federal structure. If the European Union were a single state, it would possess the world's second-largest GDP, the world's second-highest military budget, many of the world's most sophisticated defence companies, and an independent nuclear deterrent in the form of the French nuclear arsenal. From Moscow's perspective, the formation of such a military superpower on Russia's western border would be a disastrous outcome for its security interests. To reduce the likelihood of such an outcome, Russia has consistently carried out persuasive cyber operations in support of Euroskeptic politicians and movements in European states. This can be understood as part of a broader policy aimed at keeping Europe internally divided.

In cases where Russia has secured memberships in Western-dominated institutions, it often places little positive value on these memberships, perceiving them (with some justification) as constraints on its freedom of action. Russia joined the G7 in 1998 (temporarily causing the group to be renamed G8), but was expelled in response to its 2014 annexation of Crimea. Additionally, Russia joined the Council of Europe, which facilitates European cooperation on human rights issues, in 1996. It applied to join the GATT in 1993 and became a member of the WTO in 2012, effectively formalising its entry into the global capitalist economic system. However, in 2022, following its invasion of Ukraine, Russia was expelled from the Council of Europe and withdrew from both the WTO and the WHO. When faced with the choice between participating in Western-dominated international institutions and preserving its freedom to pursue self-defined foreign policy interests, Russia consistently chooses the latter.

Russia has also established its own institutions; however, the motivations behind their creation are primarily negative. During the Cold War, the Soviet Union formed Soviet-dominated institutions within the communist bloc, such as the Warsaw Pact, a security alliance, and the Council for Mutual Economic Assistance (COMECON) for economic cooperation. However, Russia's main objective was not to build strong, enduring institutions, but to counterbalance the influence of the United States and undermine American initiatives such as the Marshall Plan and NATO (Zubok, 2009, pp. 78, 102). In the post-Cold War era, Russia has participated in the creation of new institutions such as the Eurasian Economic Union (EAEU), the SCO, and the BRICS group. These institutions help to safeguard Russia from diplomatic isolation by the West and enhance its international prestige. However, Russia's broader approach to international institutions indicates that its participation is driven by fundamentally negative motivations, focusing on countering the influence of Western-dominated institutions (Stronski & Sokolsky, 2020). In general, Russia seeks to undermine institutions that impose constraints on its freedom of action, rather than to establish strong, Russian-dominated counterparts.

These negative institutional preferences set Russia apart from major powers of the Global South, such as Brazil and China. While these states are, in some respects, institutional revisionists, their institutional preferences are nevertheless positive: they seek to advance their national interests by bolstering new institutions to promote regional leadership and change the global balance of economic power. For example, Brazil wishes to strengthen MERCOSUR to promote Brazilian economic leadership in South America, while China uses the Belt and Road Initiative to establish

economic linkages with Central Asia and integrate the region into a Chinese-dominated economic system. By contrast, it seems unlikely that Russia would support an outcome in which BRICS reached the same prominence as the G7, the EAEU achieved the same level of regional integration as the EU, or the SCO developed into a tightly coordinated security alliance resembling NATO. Russia would likely be hesitant to empower these new institutions to a degree where they, too, would constrain Russian sovereignty.

There is, however, one important exception to Russia's general negative preference regarding international institutions. This is the United Nations Security Council, which Russia wishes to strengthen and reinforce. The Russian views on this institution are captured in an editorial published in 2018 by Vladimir Putin published in the *New York Times.*

> The United Nations' founders understood that decisions affecting war and peace should happen only by consensus, and with America's consent the veto by Security Council permanent members was enshrined in the United Nations Charter. The profound wisdom of this has underpinned the stability of international relations for decades. No one wants the United Nations to suffer the fate of the League of Nations, which collapsed because it lacked real leverage. […] We need to use the United Nations Security Council and believe that preserving law and order in today's complex and turbulent world is one of the few ways to keep international relations from sliding into chaos. The law is still the law, and we must follow it whether we like it or not. (Putin, 2018)

The reason for Russia's positive orientation toward the UN Security Council lies in the significant influence it grants to the country. Russia derives considerable power and prestige from being one of only five states in the world with a permanent, veto-wielding membership on the council. Permanent Security Council membership helps Russia sustain its claim to great power status in international politics and informally legitimises its position as one of the world's five authorised nuclear weapon states. Moreover, Russia makes exceptionally heavy use of its veto to advance its interests and protect its allies from criticism. Since 2000, Russia has cast its veto 27 times, compared with 14 vetoes cast by the United States, 13 vetoes cast by China, and zero cast by France and the United Kingdom (S. K. Thompson, Landgren, & Romita, 2022). During this period, most of Russia's vetoes were cast over issues such as the conflicts in Syria and Ukraine. As a result, this is one of the few areas where Russia is positively committed to the institutional *status quo*, and Russia has

traditionally been a firm opponent of expanding or reforming the Security Council, especially if this would involve curtailing the use of the veto (Bourantonis & Panagiotou, 2004).

Although Russia's views on the UN Security Council are a notable exception, the country's overall stance on international institutions is predominantly negative. The primary organising principle of Russian foreign policy in the post-Cold War era has been to oppose the emergence of hostile concentrations of power on its borders. Institutions such as NATO and the EU contribute to these concentrations, which has led Russia to adopt negative institutional preferences in its foreign policy. Furthermore, due to the offence-dominant nature of persuasive cyber operations, this type of cyber power is particularly useful for undermining institutions. In combination, these factors provide Russia with strong incentives to aggressively use persuasive cyber power in ways that undermine trust in these institutions from within. Thus, it is Russia's negative institutional preferences that explain its aggressive use of persuasive power.

6.6 Conclusion

Russia's cyber strategy can be defined by two main features: its aggressive use of technical cyber power and its equally aggressive use of persuasive cyber power. Russia's technical cyber operations are unusual, but not unique. Some of Russia's notable technical cyber operations include its use of large-scale DDoS attacks against the Baltic States; its sabotage of Ukrainian critical infrastructure; and its use of cyber espionage against the United States. Again, it should be stressed that these operations are unusually aggressive, but not exceptional. Russia's use of cyber espionage and sabotage is similar in kind – although not necessarily in its level of technical sophistication – to cyber operations carried out by the United States, as described in Chapter Five of this study. However, the more unusual aspect of Russia's cyber strategy is its aggressive and destabilising use of persuasive cyber power. Russia has used persuasive cyber operations to amplify political divisions and erode institutional trust within the United States and the European Union, in ways that are qualitatively distinct from the other states considered in this study.

Russia's principal goal in all these operations is to prevent hostile concentrations of power from forming and to create disunity within existing power concentrations that it regards as hostile. This can be seen most vividly in Russian disinformation campaigns against the United States, which have sought to strengthen centrifugal political forces that weaken the centre-left and the centre-right. This tendency also explains Russian support for regional secession movements in Scotland, Catalonia, California, Texas, and elsewhere. Defensively, Russia's persuasive cyber strategy seeks to

limit the ability of citizens to import ideas from foreign sources and reduce Russia's vulnerability to similar tactics employed by other states.

By adopting this strategy, Russia has had to make several important trade-offs. It has accepted economic costs, the risk of provoking balancing behaviour by other states, and the risk of creating a loss of trust in international institutions as well as Russia's domestic institutions. However, Russia has been willing to accept these trade-offs. This can be seen from the unusual nature of certain Russian cyber operations. Some of Russia's persuasive cyber operations have been targeted towards fairly narrow interests – for example, using Twitter bots to promote political narratives that are critical of NATO among right-wing audiences in the United States – but others have advanced surreal claims that seemingly do not advance any Russian interests directly, and instead only serve to erode trust within target states.

There are two main reasons why Russia has adopted this strategy. Firstly, Russia perceives itself as having high external security requirements. Russia has large, poor-defensible geographic borders, and has been subjected to repeated foreign invasions throughout its history. To overcome this weakness, Russian policymakers have historically sought to increase Russia's strategic depth by expanding its borders outwards; or, failing this, have at least tried to ensure the existence of friendly governments within nearby states. However, constrained by limited economic and military resources in the post-Cold War era, and unable to match the conventional strength of the United States and Western Europe, Russian policymakers have instead made use of a variety of unconventional tactics as force multipliers. This explains Russia's heavy use of cyber operations, as well as its use of a variety of other "grey zone" tactics in its international conflicts. Secondly, Russia holds negative institutional preferences. Russian foreign policy is ambivalent towards international institutions in general, and is exceptionally hostile to the two main institutions in its immediate region of Europe: NATO and the EU. These two institutions have been the main targets of Russian disinformation campaigns.

These two variables – high external security requirements and negative institutional preferences – thus provide a clear and parsimonious explanation for Russia's unusual cyber strategy. Furthermore, this explanation is congruent with the theoretical explanations for Brazil's cyber strategy and the United States' cyber strategy elsewhere in this study. The final chapter of this study considers the lessons from all these case studies in combination with each other and develops a general theory of strategy selection in the cyber domain.

Chapter 7
Conclusion: The Future of Cyber Power

7.1 Introduction

Cyber power has changed the way sovereign states play the game of international politics. It provides them with new and unconventional tools that they can use to advance their national interests. These tools enable states to act without clear attribution, undermine trust in social and technical systems, influence decision-making calculations by other states, weaken institutions, and disrupt the social cohesion of their adversaries. However, while many states now possess the capability to use these tools, they have made radically different choices about whether to do so. Most states seem to voluntarily abstain from carrying out offensive cyber operations entirely. Some have embraced cyber power with ruthless disregard for potential negative consequences, employing computer hacking and online propaganda to sabotage, subvert, and spy on their adversaries. Other states have opted for a mixed approach, using some of the tools of cyber power aggressively while exercising restraint with others. This discrepancy between strategic choices in the cyber domain is the key research puzzle that has motivated this study.

To solve this puzzle, this study develops a realist theory of cyber power. It examines the key features and limitations of cyber power and establishes a typology of four ideal-type strategies for classifying states in the real world. These include the restrained strategy, characterised by minimal use of cyber operations; the technical-aggressive strategy, focusing on cyber espionage and sabotage; the persuasive-aggressive strategy, emphasising online propaganda and disinformation; and the combined-aggressive strategy, which employs a mixture of these tactics.

This theory seeks to explain why states choose one strategy over others, and attempts to identify the specific variables that are associated with the strategy selection. Drawing from the assumptions inherent in the realist paradigm of international relations, this theory assumes that states will generally have rational and self-interested reasons for adopting a particular cyber strategy over other possible options. In particular, the study argues that two main variables explain this strategic choice. The first variable is the severity of a state's external security requirements. The second variable is the state's preference for either building institutions that serve its national interests, or weakening institutions that hinder its interests. In combination, these two variables provide a compelling and parsimonious explanation for the selection of its cyber strategy. By applying this

theory, we can explain why states adopt the strategies they do – and perhaps predict how those strategies might evolve if those circumstances were to change.

7.2 Limitations of the Findings

Before discussing the main findings of this study, it is important to acknowledge some of the limitations of this investigation.

Firstly, the primary evidence supporting the theory of cyber power presented in this study is drawn from qualitative research on three cases: the cyber strategies of Brazil, the United States, and Russia. Each of these cases encompasses multiple observations, as cyber strategies have evolved within each country. These multiple observations within the individual cases offer greater support for the theory, increasing the reliability and explanatory leverage of this research. However, the potential issue of selection bias and the limited sample size remains a concern. It is possible that there are other states whose cyber strategies might contradict the theory described in this volume if detailed case study research were to be conducted on them. Future case studies and large-n studies have the potential to provide additional tests for the theory presented herein.

Secondly, it is important to reiterate that the explanations and predictions derived from this theory are contingent and probabilistic. This theory predicts that states with certain characteristics will be more inclined towards adopting particular cyber strategies, but it does not assert that there will be absolute adherence to these strategies in every possible circumstance. Policy decision-making is invariably influenced by human agency, chance, and other unforeseen factors that introduce complexity in the causal relationships described in these chapters. As such, the predictions derived from any theory of foreign policy can never be as reliable as predictions made in the natural sciences.

Thirdly, the theory presented in this study primarily focuses on overarching patterns and high-level strategies of states. The theory is not designed to make predictions at a more granular level, and it cannot explain why specific cyber operations occur. Instead, it aims to explain the broader strategic framework that informs the decision to carry out particular cyber operations. As such, this theory does not eliminate the need for case study research that examines the details of individual cyber operations. On the contrary, research on individual operations should be considered complementary to the theory presented here, helping to explain how individual operations align with – or diverge from – the larger strategic objectives of states.

Fourthly, this study is based on information available in the public domain. This data is sourced primarily from investigative journalism, incident reports, research institutes, scholarship, and public reports from governments. This study makes an epistemological assumption that the information published by reputable journalists and cyber security experts is generally reliable. However, it is important to note that these sources are ultimately trying to make inferences about information that is kept secret and, therefore, it is unlikely that they will be perfectly accurate. The most reliable data would come from internal decision-making records of the governments of the United States, Russia, and Brazil, but these are generally classified and inaccessible to researchers. Some of this information eventually makes its way into the public domain through leaks and incident reports; however, if some information is leaked while other information remains secret, this increases the risk of bias.

Despite these limitations, every effort has been made to ensure the quality and rigour of the research. Data has been drawn from the most reliable sources available in the public domain and has been triangulated and cross-referenced across multiple sources whenever possible. Every effort has been made to avoid drawing conclusions beyond what the evidence supports. Although the theory presented here cannot make predictions as accurate as theories in the natural sciences, it can nonetheless provide valuable insights into the forces that shape cyber strategy and help to offer valuable insight into this important issue in international affairs. With these considerations in mind, we can now consider the main findings of the study.

7.3 Main Findings

Chapter One of this study begins with two research questions:

1. What are the distinct features of cyber power as a tool of foreign policy, and what are the possible strategies that states can adopt to take advantage of cyber power?
2. What are the factors and variables that influence a state's choice of cyber strategy, and how can these be integrated into a theoretical framework to explain and predict which cyber strategies a particular state will adopt?

Having now explored the theoretical limitations of cyber power, and having conducted three empirical case studies on the cyber strategies of states, we can now answer these questions.

Cyber power can be conceptually divided into two fundamental types: technical cyber power and persuasive cyber power. Technical cyber power refers to a state's ability to infiltrate electronic networks for sabotage and espionage purposes. Its use serves to erode the adversary's trust in their technical systems. Persuasive cyber power, on the other hand, involves a state's ability to convey messages to domestic audiences in targeted states to harm social cohesion and foster disunity. The use of persuasive cyber power serves to erode the adversary's political and epistemic institutions. Both forms of cyber power can be potent tools in the hands of ruthless states. They enable governments to reach beyond their borders and inflict harm upon their adversaries at a distance, without resorting to destructive wars or costly economic sanctions.

However, both forms of cyber power come with significant disadvantages and trade-offs associated with their use. States that engage in reckless cyber operations risk inciting blowback and balancing behaviour from other states, inadvertently harming their domestic economy, and eroding trust within their own societies, as well as those of their adversaries. When states make repeated choices regarding which sets of trade-offs they are willing to accept in the cyber domain, patterns in their behaviour become apparent, making it possible to discern their underlying strategies. This study is based on the underlying assumption that states can be usefully modelled as rational actors, which implies that they will attempt to avoid costs and trade-offs as much as possible. This does not mean that every foreign policy decision made by a particular government is rational; however, it suggests that state behaviour, when viewed in aggregate, will tend towards self-interest over time. If we observe a specific state repeatedly and aggressively using cyber operations over many years, we can reasonably infer that policymakers within that state believe that their aggressive strategy provides benefits that outweigh the resulting trade-offs.

This study hypothesises that states with high external security requirements will likely have insufficient resources to satisfy their security pressures through conventional military spending, making them more likely to resort to non-conventional force multipliers such as technical cyber operations. It also argues that persuasive cyber power is offence-dominant: It is useful for breaking down trust in established institutions, but less effective for enhancing or creating trust. Therefore, it hypothesises that states with positive institutional preferences, which benefit from and seek to maintain existing institutions, are less likely to use this tool, while states with negative institutional preferences, which aim to undermine or dismantle existing institutions, will gain more utility from doing so and are more likely to use it. A comparison of the three cases examined in this study – Brazil, the United States, and Russia – offers evidence and support for both hypotheses, while also

illustrating the strengths and weaknesses of each of the different cyber strategies. Let us now consider each of these cases in turn.

7.3.1 Brazil: The Restrained Strategy

Among the four ideal-type strategies identified in this study, Brazil's cyber strategy closely resembles the restrained strategy. It has a large constellation of security and intelligence agencies with expertise in cyber security and clearly has sufficient resources to carry out technical cyber operations against other states if desired. However, Brazil has consistently refrained from using its technical cyber capabilities against other states and does not actively interfere with the domestic information markets of other countries.

This restrained strategy offers important advantages for states that adopt it, ensuring that their approach to the use of both technical and persuasive cyber power is aligned with the goal of increasing societal trust. By focusing on defensive cyber security measures, a state adopting this strategy can enhance individual privacy, ensure that any software vulnerabilities it discovers are disclosed and patched, and promote norms of self-restraint internationally. This approach also benefits the state's economy by reducing online transaction costs and encouraging the development of firms and business models that make effective use of information and communication technology. Furthermore, this strategy promotes social cohesion by promoting higher levels of epistemic trust. This model encourages citizens to freely exchange ideas and engage in online civic debates, without having to fear that they are interacting with government-created personas. However, while the restrained strategy offers many advantages, it also has certain drawbacks. Most notably, the state sacrifices potential utility by not fully exploiting its cyber power to undermine adversaries' technical systems and epistemic institutions. In effect, a state choosing to adopt the restrained strategy must be willing to leave some of its potential capabilities on the table.

What type of state is likely to adopt such a strategy? This study hypothesises that there are two unit-level variables likely associated with this strategy selection: low security requirements and positive institutional preferences. Indeed, we see that both variables are present in the case of Brazil.

Brazil's low external security requirements can be attributed to its defensible geography, the absence of strong regional rivals, and the lack of major overseas commitments. Brazil's urban core in the southern cone is protected by barriers such as the Amazon rainforest and the Atlantic Ocean, which provide strong natural defences against potential attackers. The absence of extensive

overseas commitments further reduces Brazil's security requirements, as it means that its military does not need to project power or defend its interests beyond its immediate region. Furthermore, as the most powerful state in South America, Brazil does not face immediate threats from neighbouring countries. Therefore, despite its low level of military spending, Brazil appears to be relatively secure. Since Brazil can meet its security requirements through conventional measures, the marginal security gains it would receive from carrying out aggressive technical cyber operations would be low. Given the low payoff, it is rational for Brazil to avoid paying the trade-offs associated with an aggressive cyber strategy and instead focus on defence and resilience in the cyber domain.

Brazil has also played an important role in the creation and strengthening of international institutions that advance its national interests, including MERCOSUR, PROSUR, BRICS, and the G20. Brazil's institutional preferences changed somewhat during the four years of the Bolsonaro presidency, from 2019 to 2022, but this change was not strong or sustained enough to alter Brazil's cyber strategy. As such, the case of Brazil is also consistent with the second hypothesis of this study, which is that states with positive institutional preferences will find less value in using persuasive cyber power. Since the persuasive cyber domain is offence-dominant, persuasive cyber operations are more useful for eroding trust in institutions and authorities than for building trust but are not very effective at creating or maintaining trust. Since Brazil has a positive commitment to strengthening and creating institutions, it has little to gain from using this tool, and thus has rationally refrained from using it.

7.3.2 The United States: The Technical-Aggressive Strategy

Among the four ideal-type strategies identified in this study, the technical-aggressive strategy is the one that most resembles the strategy adopted by the United States of America. The United States is exceptionally aggressive in its use of technical cyber power, conducting frequent and highly sophisticated cyber operations to sabotage and spy on its adversaries. However, it does not appear to be engaged in large-scale disinformation campaigns aimed at undermining institutional trust. The United States has attempted to export its model of domestic internet regulation, and it carries out overt public diplomacy campaigns using online channels. However, it seems to place a relatively high value on maintaining epistemic trust within its domestic information market and does not want to flood these online networks with disinformation.

In contrast to Brazil's restrained strategy, the United States' technical-aggressive approach offers a powerful tool for pursuing foreign policy objectives through technical cyber operations. A state that

adopts this strategy is well placed to conduct far-reaching espionage and surveillance operations, launch destructive cyber attacks, and support its conventional military operations with cyber campaigns. In certain circumstances, these tools can significantly impact the state's ability to achieve its foreign policy goals. Furthermore, since it refrains from seeding deceptive narratives in its information market, the state aims to maintain social cohesion. Such a state may hope to promote trustworthy online civic discussions among citizens, so it avoids poisoning online dialogue by flooding it with fabricated disinformation. However, this strategy also has major risks and disadvantages. The core issue with the technical-aggressive approach is the inherent trade-off between the state's technical cyber capabilities and its civilian network security. A state that wishes to increase its offensive cyber capability must accept some vulnerability in its civilian networks, thereby reducing overall cyber security and potentially harming the state's economic interests. Additionally, even if such a state refrains from carrying out persuasive cyber operations, the use of online surveillance serves to erode individual privacy and risks reducing the state's domestic legitimacy and social cohesion. Consequently, a state that adopts this approach must be willing to accept a trade-off in the form of reduced trust in its domestic networks.

What type of state is likely to adopt a technical-aggressive strategy? This study hypothesises that two unit-level variables are likely to encourage the selection of this strategy, despite its disadvantages: high security requirements and positive institutional preferences. Both variables can be observed in the case of the United States.

The United States has exceptionally high external security requirements, despite the benefits of its highly defensible geographic position. These security requirements stem from the vast scope of its interests and its unique, quasi-hegemonic position in the post-World War II international system. In this period, the United States has maintained a large network of client states and alliance partners, positioning itself as the guarantor of the global trade and finance system. To defend this system, the United States maintains extremely high levels of military expenditure, supporting a military presence that spans the globe. However, even with this large and well-funded military, the United States has struggled to meet its various international challenges. From the early 2000s onwards, the United States has faced an array of challenges, including wars with asymmetric non-state actors such as Al Qaeda and ISIS, and security competition with hostile states such as Iran, North Korea, Russia, and China. In the face of these security pressures, the US has been more inclined to accept the trade-offs associated with the aggressive use of technical cyber power. As a result, the United States has acquired a useful tool that can be used to collect massive volumes of intelligence on its adversaries

and threaten the technical infrastructure of rival states. The sharpest growth in American cyber power occurred during periods in which the security pressures facing it were most severe: in particular, the period from 2006 to 2008 when the United States simultaneously faced the prospect of a military collapse in Iraq and the development of nuclear weapons by Iran.

With some exceptions, the United States also tends to have broadly positive institutional preferences. It is heavily invested in the existing international institutions that organise the global economy and security system, such as the WTO, the IMF, the European Union, and NATO. Although complaints about international institutions are a common feature in American domestic discourse, especially on the political right, we can observe that in practice, the United States generally wishes to maintain this system. Thus, the case of the United States is consistent with the second hypothesis of this study: countries with positive institutional preferences have less incentive to make aggressive use of persuasive cyber power and, therefore, tend not to use it.

7.3.3 Russia: The Combined-Aggressive Strategy

In contrast to Brazil and the United States, Russia's cyber strategy most closely resembles the fourth ideal-type strategy identified in this study, the combined aggressive strategy. This approach makes aggressive use of technical cyber operations in conjunction with the active projection of persuasive cyber power into other states. This strategy is unusual and Russia is likely the only state in the world that uses it fully. In periods of relative peace, Russia uses technical cyber operations as a signalling mechanism to demonstrate its resolve and intention to escalate issues where it feels its key interests are at stake. During periods of war, it uses technical cyber operations to complement its conventional military forces. Additionally, Russia actively employs persuasive cyber operations to transmit ideas to foreign audiences, disrupting social cohesion and institutional trust within the states it targets.

The primary advantage of the combined-aggressive strategy is that it enables Russia to exert additional influence through its foreign policy. By leveraging its ability to hack critical infrastructure, cast doubt on election legitimacy, amplify political divisions, and reduce institutional trust in other states, Russia gains a versatile set of tools for various foreign policy problems. Russia employs these cyber operations alongside non-traditional and asymmetric methods, including covert operations, economic statecraft, "frozen conflicts", propaganda via channels like RT and Sputnik, and an opaque nuclear posture. These approaches allow Russia to pursue a more ambitious foreign policy agenda than its economy and population would typically support. However, this strategy also carries

enormous risks and costs. The intensive use of persuasive cyber power has coincided with dismal trust levels among ordinary Russians, hindering the state's ability to create a cohesive, high-trust society. The widespread use of technical exploits has hampered the competitiveness of Russian companies in overseas markets. Furthermore, this strategy risks provoking balancing behaviour and retaliation on the part of other states. Russia's efforts to undermine NATO and the European Union through persuasive cyber power have significantly worsened relations with European countries and the United States, eliminating any chance of a *rapprochement* or a "reset" between the two sides. In summary, this high-risk strategy involves significant trade-offs.

What sort of state is likely to adopt a combined-aggressive strategy? This study hypothesises that there are two unit-level variables associated with the combined-aggressive strategy: high security requirements and negative institutional preferences. Both variables are both present in the case of Russia.

Russia's high security requirements arise from its geographic vulnerability, extensive and poorly defensible borders, proximity to powerful rival states, and ongoing territorial disputes with regional states such as Georgia and Ukraine. In the post-Cold War era, Russian foreign policy has attempted to address this issue by maintaining a sphere of influence within its region. However, this approach has put Russia on a collision course with Eastern European and ex-Soviet states that prefer closer alignment with the West, stretching the resources of the Russian military. To compensate for these military limitations, Russia has frequently relied on unconventional methods such as cyber operations. As Russia's security requirements have increased, its use of technical cyber power has become more aggressive. Following the 2008 Munich Security Conference, which signalled a shift in Russian strategic thinking, Russia began employing large-scale cyber operations against countries like Estonia and Georgia. This trend intensified after the 2014 annexation of Crimea and the subsequent imposition of sanctions by Western countries. In the face of these increased security pressures, Russian cyber operations became even more belligerent, targeting civilian infrastructure such as Ukrainian power plants. This pattern indicates a clear relationship between security requirements and cyber strategy: in periods when Russia has faced heightened security requirements, its use of cyber operations has intensified.

Russia exhibits largely negative institutional preferences, in contrast to Brazil and the United States. Instead of creating or strengthening institutions that advance its interests, Russia prioritises the goal of challenging and undermining existing institutions that it perceives as unfavourable. This is

particularly evident in Europe, where Russia feels threatened by the dominance of institutions such as NATO and the European Union. Russia resents the influence of the United States in its near-abroad region and fears the prospect of a politically unified and militarily powerful Europe. Consequently, Russia has aggressively employed persuasive cyber operations to promote political candidates and movements hostile toward these institutions, such as Donald Trump and the "alt-right" movement in the United States, Marine Le Pen in France, and possibly the Vote Leave campaign during the 2016 Brexit referendum in the United Kingdom. There is a discernible link between Russia's use of persuasive cyber power and its desire to challenge the existing institutional landscape in Europe.

		External Security Requirements	
		Low	High
Institutional Preferences	Positive	**"RESTRAINED STRATEGY"** Restrained use of technical cyber power Restrained use of persuasive cyber power **BRAZIL**	**"TECHNICAL-AGGRESSIVE STRATEGY"** Aggressive use of technical cyber power Restrained use of persuasive cyber power **U.S.A.**
	Negative	**"PERSUASIVE-AGGRESSIVE STRATEGY"** Restrained use of technical cyber power Aggressive use of persuasive cyber power	**"COMBINED-AGGRESSIVE STRATEGY"** Aggressive use of technical cyber power Aggressive use of persuasive cyber power **RUSSIA**

Figure 9: Summary of the overall findings of this study.

7.4 Predictions that Flow from this Theory

This study develops a realist theory of cyber power, arguing that a state's choice of cyber strategy is influenced by external security requirements and institutional preferences. Analysis of the three cases – Brazil, the United States, and Russia – supports this theory. Beyond these specific cases, the theory offers a general framework for understanding cyber strategy that is applicable to all states, and provides insight into how states might alter their strategies in response to changing circumstances. Although this theory seeks to be predictive, it cannot offer the precision found in predictions within the natural sciences. Instead, it can state in probabilistic terms that states with specific characteristics are more likely to adopt particular cyber strategies. In this final section of the volume, the theory's predictive power will be tested by examining potential shifts in state cyber strategies in response to changes in state-level variables.

Predictions in social sciences like International Relations can be challenging due to the complexity of social phenomena. However, predictive exercises can be a valuable tool for refining and applying theoretical frameworks. As Mearsheimer (2003) notes, if we attempt to imagine new events and anticipate potential shifts, we can formulate theoretical claims without succumbing to hindsight bias. In this spirit, the following section explores six possible future scenarios involving the states examined in this study. It is important to note that the point of this exercise is not to claim that any of the scenarios presented here are likely to occur. In fact, some of these scenarios are quite speculative and would require significant political changes. The goal is not to predict what will happen in these countries, but instead to make contingent predictions about how their cyber strategies would evolve if certain underlying conditions were to change. In doing so, it is possible to illustrate the dynamic interaction between shifts in the international system and cyber strategy selection.

7.4.1 Scenario #1: Hegemonic Brazil

In this scenario, we envision a world in which Brazil has become a regional hegemon in South America. To achieve this, Brazil would have to do several things: significantly increase its economic wealth, convert some of that wealth into military power, expand its influence across the continent, establish its regional power by establishing strong economic and security institutions, and expel foreign influences from the region.

This scenario would require an extraordinary level of economic growth, which would be difficult to achieve based on Brazil's current trajectory. To make this scenario possible, we might imagine some new development that radically reshapes the global economy; for example, a breakthrough technological innovation that dramatically increases the demand for Brazil's natural resources and alters the strategic balance in the region.

This scenario would also require significant changes in Brazilian grand strategy, including a greater willingness to use its economic resources to fund military capabilities and a readiness to form a network of institutions, alliances, and client states within the region. Furthermore, it would necessitate the use of various foreign policy tools to punish states that do not wish to be part of this network. In essence, this scenario would see Brazil occupying a position in South America akin to the position currently held by the United States in North America or the position that the Soviet Union held in Eastern Europe during the Cold War.

How would Brazilian cyber strategy change in this scenario? First, a hegemonic Brazil would certainly face new security pressures if it attempted to form a regional hegemony. Such a policy would be met with pushback from other states and power centres within the region, as well as from powerful states outside of its region. Even if it invested a significant portion of its resources in its military, a hegemonic Brazil might struggle to cope with these security pressures. Consequently, it would seek ways to enhance the effectiveness of its existing foreign policy tools. For example, Brazilian security agencies that deal with defensive aspects of cyber security, such as ABIN, might be revamped to bolster their offensive cyber capabilities. Brazil would likely make extensive use of electronic espionage and surveillance to better understand its adversaries and improve the effectiveness of its foreign policy strategies. Additionally, in this scenario, Brazil might consider carrying out destructive cyber attacks to signal its intentions and resolve to its adversaries, or to directly impair their capabilities. As a result, a hegemonic Brazil would almost certainly become much more aggressive in its use of technical cyber power.

At the same time, a hegemonic Brazil would be increasingly dependent on its regional institutions to establish and entrench its influence within the region. Brazil would have to demonstrate the credibility and trustworthiness of the institutions it establishes, since these institutions would likely serve as the anchor of its regional dominance. Thus, a hegemonic Brazil would probably refrain from using persuasive cyber operations, since these activities could undermine the legitimacy of the very institutions it would seek to promote.

In combination, these two choices – aggressive use of technical cyber capabilities, and a commitment to avoiding persuasive cyber operations that could erode institutional trust – would probably lead a hegemonic Brazil to adopt a technical-aggressive cyber strategy. This approach would allow Brazil to advance its security interests while simultaneously maintaining the credibility and legitimacy of the regional institutions that would be necessary to underpin its status as a regional hegemon.

7.4.2 Scenario #2: Brazil Under Siege

This scenario imagines a future in which Brazil has become an international pariah state, possessing few allies, and facing a large coalition of enemies. This scenario seems unlikely, as Brazil has historically enjoyed cooperative relations with most states. However, to make such a scenario possible, we might envision a future Brazilian government determined to exploit the economic potential of the Amazon basin, resulting in increased global climate change and creating insecurity for other states. Since a policy of deforesting the Amazon could create economic benefits for Brazil while imposing economic and environmental costs on the rest of the world, this action could create game-theoretical incentives for conflict between Brazil and other states.

In response, other states might seek to create international institutions, such as "climate clubs," to address the issue. These clubs would consist of groups of countries collaborating on climate change mitigation policies, with the aim of facilitating cooperation on climate change issues while imposing costs on countries outside the club (Keohane & Victor, 2016, p. 573). In a world where climate change has become a pressing international security concern, other states may even form international alliances or coalitions to stop Brazil's deforestation policy through coercive diplomacy.

How would Brazilian cyber strategy evolve under these circumstances? In this world, Brazil would face a much more threatening international environment, leading to dramatically increased external security pressures. Although Brazil would still have the advantage of a defensible geographic position in the southern cone, the existence of a hostile coalition of states would force Brazil to significantly increase its level of military spending, straining its resources. As in Scenario #1, we might expect that if Brazil found itself in this position, it would aggressively employ technical cyber operations to try to offset this constraint.

Furthermore, with few allies and faced with a hostile international community, Brazil would quickly realise that a policy of creating and strengthening international institutions would no longer serve its interests. As a consequence, Brazil's institutional preferences would likely become increasingly

negative, with Brazilian strategy focusing on undermining and challenging the existing institutional order. To erode trust in institutional frameworks that Brazil no longer deemed beneficial, the country would likely begin to use persuasive cyber power to sabotage international institutions. For instance, we might imagine Brazil employing persuasive cyber operations to attack the scientific consensus on climate change or to sow public distrust in international environmental regulations. Consequently, a "siege" scenario would likely prompt Brazil to adopt a combined-aggressive cyber strategy, encompassing both offensive technical cyber capabilities and persuasive operations aimed at undermining adversaries and their institutions.

7.4.3 Scenario #3: Revisionist United States

This third scenario imagines a world in which the United States has decided that the post-World War II "liberal international order" no longer serves its interests and decides to leave it. This would represent a significant shift in US foreign policy, which was strongly involved in the creation of institutions such as NATO, the World Bank, the IMF, the WTO, and the UN Security Council. The United States has even fought wars to protect it – the 1991 Gulf War, for example, was fought explicitly in defence of this institutional order.

However, as the balance of power in the international system has shifted, we have seen the emergence of populist and revisionist views on foreign policy within the United States. The peak of this trend was the "America First" foreign policy of Donald Trump, which dramatically altered US foreign policy toward institutions. On Trump's first day in office, the United States withdrew from the TPP, an attempt to create a U.S.-dominated institutional order in the Asia-Pacific region. Under Trump, the United States significantly reduced its cooperation with European allies, withdrew from the World Health Organisation, threatened to withdraw from the WTO, withdrew from and renegotiated NAFTA, withdrew from the JCPOA that had previously regulated the Iranian nuclear programme, and privately considered withdrawing from NATO. Some of these decisions have been wholly or partially reversed by the Biden Administration. However, several others, such as the withdrawal of the United States from the TPP, have remained in force.

Currently, the future of the United States' commitment to the institutional *status quo* is an open question. Future historians will view the foreign policies of the Trump administration as a temporary anomaly, brought about by an unusual confluence of personal and political factors that caused Donald Trump's rise to power. However, it is also possible that the Trump Administration will be seen as the beginning of a new phase in US foreign policy: the point at which the United States first

realised that the changing balance of power meant that the "liberal international order" no longer suited its interests and began its long shift towards negative institutional preferences.

In this scenario, we can imagine a situation in which US leaders are determined to maintain their country's position as the world's dominant military power and have concluded that the liberal international order constrains America's interests rather than advancing them. Such a situation might arise due to American frustration with China's economic growth, which has been enabled by the global system of free trade conducted under the rules of the WTO. American policymakers might become resentful of WTO rules that prevent them from pursuing policies of economic nationalism. They might also resent NATO for compelling the US to subsidise the defence of the European Union, which they now view as a rival rather than a partner. In this world, the "America First" doctrines of the Trump Administration would essentially become the new conventional wisdom among US foreign policy elites.

If the United States were determined to maintain its position of military dominance in such a world, its high external security requirements would potentially increase even further. Without the institutional veneer that makes US hegemony acceptable to other nations, the stark reality of American dominance would likely face greater opposition, prompting balancing strategies from other states. Such a scenario could place additional strain on its conventional military resources, leading US policymakers to seek additional tools to expand their foreign policy options, such as new forms of cyber operations.

In this scenario, a revisionist United States would likely begin to conduct increasingly aggressive persuasive cyber operations, similar to those carried out by Russia under the presidency of Vladimir Putin. These operations could target a variety of objectives. For example, the US might use persuasive cyber operations to create internal divisions within hostile states, potentially destabilising their political systems and weakening their ability to challenge American interests. Additionally, the United States could employ such tactics to sow discord within opposing coalitions of states, undermining their unity and effectiveness in countering US influence. Another potential target of this revised cyber strategy would be the international institutions that the US perceives as constraining. By weakening these institutions and eroding trust in them, a revisionist United States could gain greater freedom to pursue its objectives without being burdened by institutional constraints. In this world, the US would actively seek to foster distrust and uncertainty within the international community, further destabilising the existing order. Due to this combination of high

security pressures and a desire to dismantle the institutional *status quo*, a revisionist United States would likely adopt the combined-aggressive cyber strategy.

7.4.4. Scenario #4: Neo-Isolationist United States

An alternative scenario for the United States imagines a world in which it has retreated towards "neo-isolationism", rather than aggressive revisionism. Historically, isolationism has played a significant role in American foreign policy. The country's first president, George Washington (1796), urged his successors to "steer clear of permanent alliance with any portion of the foreign world" . Throughout much of its early history, the United States was torn between the impulse to establish regional hegemony and the desire to isolate itself from "entangling alliances" with the Old World. Although the US never fully committed to either path, isolationism remained influential in American foreign policy until the end of World War II. Even in the latter half of the twentieth century, neo-isolationist positions were advocated by a small number of Republican politicians, such as Robert Taft and Pat Buchanan.

Today, the United States has established an extraordinary network of alliances and institutions that shape its foreign policy, making it unlikely that the United States would return to isolationism. However, the desire for retrenchment from foreign commitments has never completely disappeared from the American body politic. In right-wing politics, it has become fashionable to criticise "globalism," and within this discourse, elements of the old isolationism can be seen reasserting themselves.

In this scenario, we can define "neo-isolationism" as a foreign policy based on the idea of significantly reducing the United States' external security requirements. We might envision a future where operational failures abroad, war-weariness among the public in general, and fiscal constraints on military spending have led the US to drastically downscale its security commitments to other states. In the contemporary globalised world, it is impossible for any state to completely disengage from international trade or environmental politics. However, there is potential for the United States to significantly reduce its current security requirements. We can envision a world where the US withdraws from NATO, revokes many of its security guarantees from non-NATO allies, and reduces its military spending to a level comparable with other large states such as China. In such a world, the US might not fully disengage from security commitments; instead, it could opt for a grand strategy of offshore balancing, selectively allying itself to prevent dangerous concentrations of power from

forming in other regions of the world, while declining to form permanent alliances or create networks of client states.

How would the US cyber strategy evolve in such a neo-isolationist scenario? In the short term, this change in grand strategy would significantly reduce the United States' external security pressures. As a large continental power, protected by vast oceans and with no strong adversaries in its immediate region, a neo-isolationist United States would be able to considerably reduce its military expenditure while still effectively defending its homeland. With a scaled-back overseas presence and fewer security commitments, a neo-isolationist US would find itself in a position where aggressive technical cyber operations against other states would become less necessary. Instead, the focus could shift toward bolstering its defensive capabilities to protect critical infrastructure and domestic networks, as well as investing in deterrence measures to discourage potential adversaries from launching cyber attacks on the US. In this scenario, the trade-offs of an aggressive technical cyber strategy – weakened cyber security, economic costs to US businesses, and the possibility of retaliation from other states – would appear more acute in a world where the US has less need for these capabilities. Thus, it is likely that a neo-isolationist United States would adopt a restrained cyber strategy.

7.4.5. Scenario #5: Status Quo Russia

The next scenario to consider is one in which Russia adopts positive institutional preferences. Although this would be historically unusual, it would not be unprecedented. At various points in its history, Russia has strongly favoured the institutional *status quo*. For instance, following the Napoleonic Wars in 1815, Russia formed the Holy Alliance with Austria and Prussia to protect the conservative *status quo* in European politics. During this period, the Russian Empire intervened repeatedly to defend other European monarchies against republican and democratic revolutions, earning the nickname "the policeman of Europe." In the aftermath of the Cold War, Russia initially pursued a policy of accommodation and *rapprochement* with Western democracies under President Boris Yeltsin and Foreign Minister Andrei Kozyrev. During this time, Russia agreed to German reunification, signed the Budapest Memorandum promising to respect Ukraine's territorial integrity, and joined the Council of Europe. However, this policy shifted after the 1997 Kosovo War and, by 2008, Russia had effectively become an adversary of the institutional *status quo* in Europe.

We might envision a future scenario in which Russia has undergone a democratic transition and has shifted away from the irredentist foreign policies and negative institutional preferences that characterised the presidency of Vladimir Putin. In this scenario, Russia has reconciled itself to the

loss of its territorial empire and has instead chosen to focus on developing a dynamic and modern economy.

As a result of this strategy, Russia's external security requirements would likely be significantly reduced. If Russia were to give up on its ambitions of maintaining a regional sphere of influence, its incentives for conflicts with neighbouring states would be sharply reduced. Russia could wind down longstanding conflicts in regions such as Ukraine and Georgia and would no longer need to maintain as large a military presence to exert influence over its region.

Consequently, Russia might find its security commitments are more achievable using conventional methods, reducing the need for aggressive technical cyber operations against adversaries. Furthermore, if Russia were to focus on developing a high-tech economy to supplement its oil and gas industries, the costs of an aggressive technical cyber strategy would become more acute. Russia would need to ensure trust in its domestic networks to facilitate a modern economy and financial system, while a policy of hoarding and using exploits would undermine that trust.

Additionally, a pro-*status quo* Russia would need to enhance trust from foreign customers of Russian services. It would aim to strengthen Russian technology companies that sell their services overseas, such as Kaspersky and Telegram, and would not want these companies to be inadvertently harmed by their association with the Russian state. In general, the benefits of carrying out aggressive technical cyber operations would diminish, and the costs of such operations would increase.

A pro-*status quo* Russia would also likely be less hostile toward international institutions such as the EU. On the contrary, it would probably see significant potential economic benefits from membership in institutions such as the EU and the European Common Market and would seek to join them. Moreover, in this scenario, Russia would need to rejoin the WTO to maintain its ability to export goods and services to other states and protect the intellectual property of its firms. Russia would likely seek to establish closer economic ties with Asian states, allowing it to benefit from commerce between Europe and Asia and serve as a bridge between the two regions. For all these reasons, Russia would probably adopt positive institutional preferences and would refrain from conducting persuasive cyber operations that undermine trust in these institutions. In general, this scenario would prompt Russia to adopt a restrained cyber strategy.

7.4.6 Scenario #6: A World of Parallel Institutions

Finally, let us consider a more complex scenario than the others described here: a world in which there are multiple sets of international institutions that exist simultaneously and compete with each other. This scenario imagines a world where the rise of China has created a bipolar international system, with two competing superpowers possessing roughly equal levels of wealth and power. Initially, China would try to increase its influence within Western-created liberal international institutions. However, if China found that it was unable to do so – perhaps due to Western recalcitrance, or perhaps because the design of these liberal institutions proved intrinsically inimical to Chinese interests and ideological preferences – it would then seek to create its own set of Chinese-dominated institutions, following the example set by the United States in the aftermath of World War II.

In this world, we would see a situation in which Chinese-sponsored institutions were strengthened and became true competitors to Western-dominated institutions. BRICS would become a true alternative to the G8; the SCO would evolve into a military alliance similar to NATO; the New Development Bank (NDB) and the Asian Infrastructure Investment Bank (AIIB) would emerge as alternatives to the World Bank; and the Belt and Road Initiative (BRI) would be transformed into an international trade area, similar to the WTO system. We might even imagine the collapse of the United Nations Security Council – perhaps in response to paralysis over the use of the widespread use of the veto by both sides – and its replacement by two successor organisations, with one being dominated by China and its allies, and the other dominated by the United States and its allies.

In this world of parallel institutions, both major powers would find themselves in a complex position. They would have both positive preferences regarding their own preferred institutions, and negative preferences regarding the institutions maintained by their adversary. When choosing their respective grand strategies, they would have to decide which preference to prioritise. If the United States and China both chose to focus on undermining their adversary's institutions, the theory in this volume predicts that they would adopt combined-aggressive strategies in the cyber domain, actively using persuasive cyber power for this purpose. In this world, we could expect to see the United States use persuasive cyber operations to influence domestic audiences in Chinese-aligned states, attempting to sow distrust in their governments and the international institutions of which they were members. For example, the US might carry out disinformation campaigns accusing Chinese-backed institutions of corruption, human rights violations, or environmental degradation. Conversely, China would likely use persuasive cyber operations to undermine trust in governments

and institutions in US-aligned states, perhaps by spreading conspiracy theories or highlighting instances of Western hypocrisy.

State	Current Independent Variables	Scenario	New Independent Variables	New Cyber Strategy
Brazil	Low Security Reqs. → Positive Institutional Prefs. →	"Hegemonic Brazil"	→ High Security Reqs. → Positive Institutional Prefs.	Technical-Aggressive
		"Brazil Under Siege"	→ High Security Reqs. → Negative Institutional Prefs.	Combined-Aggressive
USA	High Security Reqs. → Positive Institutional Prefs. →	"Revisionist USA"	→ High Security Reqs. → Negative Institutional Prefs.	Combined-Aggressive
		"Neo-Isolationist USA"	→ Low Security Reqs. → Positive Institutional Prefs.	Restrained
		"Parallel Institutions"	→ High Security Reqs. → Negative Institutional Prefs.	Combined-Aggressive
Russia	High Security Reqs. → Negative Institutional Prefs. →	"Status Quo Russia"	→ Low Security Reqs. → Positive Institutional Prefs.	Restrained

Figure 10: Summary of possible cyber strategy scenarios

In some respects, this situation would represent a return to the dynamics of the Cold War, during which superpowers used radio broadcasts and printed propaganda to undermine each other's systems from within. However, radio broadcasts could reach only a small percentage of the population. This differs significantly from our current media environment, in which the vast majority of people get their news from social media platforms, and are therefore potentially exposed to state-sponsored persuasive cyber operations. A world in which all the great powers decided to make widespread use of persuasive cyber operations could be radically destabilising: it could flood social media platforms with disinformation, drowning out legitimate news, and making it extremely difficult for people to discern the truth. These subversive operations could be algorithmically targeted at specific audiences, using data analytics and generative artificial intelligence to craft highly effective messaging that exploits pre-existing social divisions.

Thus, the theory presented here suggests that a world of parallel institutions would be a dangerous outcome. It could trigger a pattern of intense global competition between rival sets of institutions, accompanied by escalating use of persuasive cyber operations. This could have profound consequences for our collective ability to distinguish between truth and falsehood.

7.5 Contribution to the Field

Previous research on state behaviour in the cyber domain has tended to focus on describing the behaviour of individual states, documenting specific incidents, and discussing the general implications of cyber power on warfare and international politics. This study seeks to advance the discipline of International Relations by moving beyond description and idiomatic explanation, toward a systematic and theory-driven understanding of cyber strategy selection based on the identification of state-level variables. This framework avoids reliance on idiosyncratic and atheoretical explanations, and could, in principle, be applied to any country in the world. This framework provides scholars and policymakers with an analytical tool that can be used to anticipate which types of states are likely to pursue certain types of cyber strategies.

This theory is built upon an integrated conception of cyber power that includes both its technical and persuasive dimensions. This approach combines technical cyber operations (such as computer hacking) and persuasive cyber operations (such as disinformation campaigns) into a single framework that views both forms of cyber power as methods used for undermining trust in the socio-technical systems. Much of the previous research on cyber conflict has tended to treat these issues separately and to focus more heavily on technical cyber operations. By contrast, this study recognises the vital importance of trust in creating functional societies, and the potential for cyber operations to erode this trust. It offers insight into the strategic incentives that are driving cyber attacks, encouraging disinformation campaigns, and degrading epistemic and institutional trust within societies across the world.

The theory developed in this volume also sheds new light on the trade-offs associated with the use of cyber power. It draws attention to the global and interconnected nature of the internet, which makes it difficult for a state to erode trust in one part of the network without causing unintended consequences in other parts. For example, a zero-day exploit used to attack a foreign adversary can be reverse-engineered and subsequently used to infect civilian networks within the attacking state. Similarly, propagandistic narratives seeded into an adversary's social networks can return home through a process of memetic transmission, and end up undermining domestic trust in the

government that carried out the persuasive cyber operation. This insight helps explain the theoretical puzzle of why many states choose not to make use aggressive of cyber operations, even if they have the technical capability to do so.

Building on these insights, this study develops a new typology of four cyber strategies: restrained, technical-aggressive, persuasive-aggressive, and combined-aggressive. It hypothesises that the selection of a cyber strategy by states is primarily determined by two independent variables: their external security requirements and institutional preferences. In particular, states with high external security requirements are more likely to use technical cyber power aggressively, while states with negative institutional preferences are more inclined to make aggressive use of persuasive cyber power. This approach provides a parsimonious but compelling explanation for the selection of cyber strategies.

The empirical component of this study employs both congruence testing and cross-case comparison, incorporating a negative case study in its research design. Previous studies have tended to focus on states that actively engage in cyber operations, as these cases provide the most readily available data. However, this represents a form of sampling bias. As a result of this problem, there has been less scholarly interest in explaining restrained strategies, even though restrained strategies are almost certainly the mostly common approach to cyber power in the current international system. This study seeks to remedy this problem by including Brazil as a negative case: a state that tends not to use cyber power aggressively. By selecting a diverse set of cases and comparing and contrasting variables across them, this study seeks to develop a balanced and comprehensive understanding of cyber strategy selection. The findings from these empirical case studies are congruent with the expectations of the theory.

Lastly, this research has substantial policy relevance. As a generalisable theoretical framework that can be applied across various geopolitical contexts, it offers a promising tool for policymakers. This study seeks to identify the state-level variables that prompt states to carry out cyber attacks and disinformation campaigns, understanding cyber strategy as the product of external security requirements and institutional preferences. This approach not only provides explanations for past and present state behaviour but also, potentially, offers predictive insights. These insights could equip policymakers with knowledge about which countries are likely to deploy these tools, perhaps encouraging them to take pre-emptive steps to increase the stock of institutional and epistemic trust within their societies.

Overall, this study presents an original, theory-driven, and policy-relevant explanation of cyber power as a tool of foreign policy. It introduces an integrated conception of cyber power that incorporates both its technical and persuasive dimensions and considers both the potential gains as well as the costly trade-offs associated with cyber operations. The study proposes a new typology of cyber strategies and develops a robust theoretical framework that explains and predicts the selection of these strategies. As such, this study makes a significant contribution to the field of International Relations.

7.6 Avenues for Future Research

This study lays the groundwork for a theoretical understanding of how states make use of cyber power and the trade-offs they face when doing so. There are several areas where future research could build on and extend the findings of this work.

Firstly, new case studies could serve as additional tests of this theory; this would also help to further clarify the causal mechanisms involved in the selection of cyber strategies. In particular, case studies on mid-level powers and smaller states would provide an important addition to the case studies of the larger countries examined in this volume, as this would help develop a more comprehensive understanding of how states with differing levels of power engage with the cyber domain. This broader perspective could reveal new patterns and nuances in state behaviour, offer additional insight into cyber strategy selection, and help refine this theoretical framework.

Secondly, the use of quantitative, large-N studies could provide complementary evidence and help to further test the theoretical framework developed in this study. By analysing a large number of cases, researchers could identify broader patterns and trends related to the use of cyber power by states. Large-N studies could also help identify any outliers that may warrant further case study research. However, this approach would likely require the development of new tools and indices to operationalise certain theoretical concepts, such as a state's level of aggression in its use of technical and persuasive cyber power.

Thirdly, an important avenue for future research is to establish the determinants of peace and stability in the cyber domain. This could involve exploring the role of international norms and rules in promoting stability, as well as examining the potential creation of explicit systems of deterrence with clear red lines that discourage aggression. This research has established that there are certain trade-offs associated with technical and persuasive cyber power and that these trade-offs appear to

discourage many states from being overly aggressive in their use of cyber power. This suggests the validity of the view that states are, in an abstract sense, rational actors. It implies that it should be possible to adjust the rules of the game in ways that would reduce the level and intensity of inter-state cyber conflict.

Fourthly, scholars in International Relations will need to study the impact of emerging cyber technologies, such as quantum computing and generative artificial intelligence, on the dynamics of cyber power. Just as the development of the internet created the possibility of state-sanctioned cyber operations, so too will new developments in the field of computing create new tools of statecraft. For example, quantum computing has the potential to render existing cryptography models obsolete, while generative AI has the potential to create extremely convincing forms of persuasion that are tailored to exploit the psychological weaknesses of individuals. Such technological developments could dramatically alter the balance between gains and trade-offs that inform strategy selection, perhaps causing certain states to rethink their current strategy in the cyber domain.

7.7 Conclusion

There are many ways that we could try to explain the discrepancy between the cyber strategies of different states. A state's choice of cyber strategy might be attributed to its ideology, its strategic culture, its domestic regime type, or the personal whims of its leaders. While all these other factors undoubtedly play some role, this study makes the case for a simpler explanatory framework, suggesting that the differences between the cyber strategies of the three states examined here can be explained by just two factors: their external security requirements and their institutional preferences.

The logic of this explanation is straightforward. Aggressive cyber strategies tend to incur costs and trade-offs; states will rationally choose to avoid these costs unless the expected gains of an aggressive strategy are high. If a state has high external security requirements, the expected payoff from an aggressive strategy will also be higher, making the associated costs and trade-offs seem more acceptable. Such states will typically attempt to satisfy their security requirements through high levels of military expenditure, but since all states face economic constraints on military spending, they will tend to search for technological force multipliers, such as cyber operations, to provide them with an additional advantage over their adversaries. Furthermore, states with negative institutional preferences have the potential to receive a higher payoff from persuasive cyber

operations than states with positive institutional preferences. All political institutions are dependent on trust, and persuasive cyber operations are effective at eroding this trust. Since their potential payoff is higher, states that exhibit both high external security requirements and negative institutional preferences will tend to make more aggressive use of hacking and subversion as tools of foreign policy.

Of course, there are many nuances and details that this analysis omits. The theory of cyber power presented in this study helps explain the broad patterns of cyber strategy selection, but it cannot account for operational or tactical choices. For example, it does not explain why Israel opted to collaborate with the US in a cyber attack against Iran in 2009 rather than choosing another option such as an air strike, a diplomatic initiative, or simply doing nothing. Similarly, in 2015, this theory would not have been able to predict that Russia would soon launch a phishing attack against the Democratic Party of the United States, and then leak the stolen information online. However, the theory does explain why Israel, a state with high external security requirements, would develop sophisticated technical cyber capabilities and choose to make aggressive use of these capabilities. It also explains why Russia, a state with negative institutional preferences, would seek to undermine trust in pro-institutional political candidates and political movements in other countries. In this sense, this theoretical perspective can help us understand and predict the broad strategic choices that states facing particular circumstances are likely to make.

If the theory presented in this study is valid, it has several disconcerting implications. It implies that cyber conflict can be expected to rise in intensity if the general level of insecurity in the international system were to increase, or if more countries were to adopt negative institutional preferences. Unfortunately, both developments seem to be increasingly likely. The primary trend in the current international system is the shift toward multipolarity, which appears to be creating a more insecure and conflict-prone world – as demonstrated by the war in Ukraine and the increasing tensions surrounding Taiwan. Moreover, the shift toward multipolarity risks creating a world of fractured, parallel institutions. As China's economy grows, it will inevitably establish networks of institutions to promote its interests, just as the United States did after World War II. If the United States and China cannot agree on a shared institutional framework for addressing global problems – a distinct possibility – there is a danger that the great powers will begin to focus their energies on undermining each other's institutions, rather than on solving collective action problems. In combination, these trends are likely to result in a general escalation in all forms of cyber conflict.

Cyber power, in its most fundamental sense, can be understood as a state's capacity to destroy trust. The widespread use of cyber operations by states undermines trust in network security, erodes our sense of privacy, and diminishes our faith in the systems we rely on for communication and financial transactions. Pervasive surveillance operations force us to live in a panopticon, imposing the psychological burden of worrying that anything we say or do online might be recorded and used against us. Persuasive cyber operations are, in many respects, even more destructive. The spread of online propaganda by powerful actors serves to encourage conspiratorial thinking and destroys our collective perception of the truth. In its most extreme form, a world in which our communications networks were flooded with disinformation would be a world without the possibility of democracy, scientific progress, or any capacity for evidence-based problem-solving. This would be a tragic outcome for humanity.

Bibliography

Aaronson, S. A. (2017). What Might Have Been and Could Still Be: The Trans-Pacific Partnership's Potential to Encourage an Open Internet and Digital Rights. *Journal of Cyber Policy, 2*(2), 232-254.

Ablon, L., & Bogart, A. (2017). Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits. *RAND Corporation.* Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf

Acemoglu, D., & Robinson, J. A. (2012). *Why Nations Fail: The Origins of Power, Prosperity and Poverty*. London: Profile Books.

Ackerman, S. (2009). Future of Public Diplomacy Unsettled at State. *The Washington Independent.* Retrieved from https://washingtonindependent.com/30404/future-of-public-diplomacy-unsettled-at-state/

Adair, S. (2016). PowerDuke: Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs. *Volexity Blog.* Retrieved from https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/

AFP. (2020). Russia Dismisses Hacking Allegations as 'Russophobia'. *Security Week.* Retrieved from https://www.securityweek.com/russia-dismisses-hacking-allegations-russophobia

Aguilera, J. (2020). Watchdogs Say Assaults on Journalists Covering Protests Is on a 'Scale That We Have Not Seen Before'. *Time.* Retrieved from https://time.com/5846497/journalists-police-george-floyd-protests/

Aisch, G., Huang, J., & Kang, C. (2016). Dissecting the #PizzaGate Conspiracy Theories. *The New York Times.* Retrieved from https://www.nytimes.com/interactive/2016/12/10/business/media/pizzagate.html

Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics, 84*(3), 488-500.

Al Jazeera. (2019). Tankers, Drones and Tweets: Key Events in Gulf Tensions. *Al Jazeera.* Retrieved from https://www.aljazeera.com/news/2019/06/20/tankers-drones-and-tweets-key-events-in-gulf-tensions/

Al Jazeera. (2022). Russia Restricts Access to Several Western Media Websites. *Al Jazeera.* Retrieved from https://www.aljazeera.com/news/2022/3/4/russia-restricts-access-to-several-western-media-websites

Albright, D., Brannan, P., & Walrond, C. (2010). Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? *Institute for Science and International Security.* Retrieved from https://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

Allison, R. (2008). Russia Resurgent? Moscow's Campaign to 'Coerce Georgia to Peace'. *International Affairs, 84*(6), 1145-1171.

Almeida, V. (2014). NETmundial, Marco Civil and CGI.br: The Modern Brazilian Regulatory Environment for the Internet. *Internet Corporation for Assigned Names and Numbers.* Retrieved from https://archive.icann.org/meetings/losangeles2014/en/schedule/wed-ig/presentation-netmundial-marco-civil-15oct14-en.pdf

Almeida, V., Getschko, D., & Afonso, C. (2015). The Origin and Evolution of Multistakeholder Models. *IEEE Internet Computing, 19*(1), 74-79.

Almond, D., Du, X., & Vogel, A. (2020). Russian Holidays Predict Troll Activity 2015-2017. *NBER Working Paper Series.* Retrieved from http://www.nber.org/papers/w28035

Alperovitch, D. (2016). Bears in the Midst: Intrusion Into the Democratic National Committee. *CrowdStrike Blog.* Retrieved from https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Alsina Jr, J. P. S. (2017). Grand Strategy and Peace Operations: The Brazilian Case. *Revista Brasileira de Política Internacional, 60*(2), 1-22.

Amorim, C. (2011). Let Us In. *Foreign Policy.* Retrieved from https://foreignpolicy.com/2011/03/14/let-us-in/

Anderson, N. (2012). Confirmed: US and Israel Created Stuxnet, Lost Control of It. *Ars Technica.* Retrieved from https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/

Anonymous. (2012). Anonymous Attacked Dozens of Websites Protesting Rio + 20 - #Ophackinrio # Oprio20. *AnonOps Communication.* Retrieved from http://anonopsbrazil.blogspot.com/2012/06/anonymous-atacou-dezenas-de-websites-em.html

AP News. (2017). The Latest: Le Pen Vows to Pull France Out of EU, NATO. *AP News.* Retrieved from https://apnews.com/article/0bb51aea51214887ad2c2454cd54a32a

AP News. (2018). Ukrainian Authorities: We Thwarted 'Massive' Cyberattack. *Associated Press.* Retrieved from https://apnews.com/article/6eb40bb43cc74c6eb5b9e386ee62aa20

Applebaum, A. (2022). The Reason Putin Would Risk War. *The Atlantic.* Retrieved from https://www.theatlantic.com/ideas/archive/2022/02/putin-ukraine-democracy/621465/

Arnaudo, D. (2018). Brazil: Political Bot Intervention During Pivotal Events. In S. C. Woolley & P. N. Howard (Eds.), *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (pp. 128-152). Oxford: Oxford University Press.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is Coming! *Comparative Strategy, 12*(2), 141-165.

Arquilla, J., & Ronfeldt, D. (1996). *The Advent of Netwar*. Santa Monica: RAND Corporation.

Arquilla, J., & Ronfeldt, D. (1997a). *Swarming and the Future of Conflict*. Santa Monica: RAND Corporation.

Arquilla, J., & Ronfeldt, D. (Eds.). (1997b). *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica: RAND Corporation.

Arquilla, J., & Ronfeldt, D. (Eds.). (2001). *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica: RAND Corporation.

Arsène, S. (2016). Global Internet Governance in Chinese Academic Literature: Rebalancing a Hegemonic World Order? *China Perspectives, 2016*(2), 25-35.

Article 19. (2009). Brazil: Proposed Electoral Law Restricts Internet Freedom. *Free Word Centre.* Retrieved from https://www.article19.org/data/files/pdfs/press/brazil-proposed-electoral-law-restricts-internet-freedom.pdf

Ash, T. G. (2010). *Cold War Broadcasting: Impact on the Soviet Union and Eastern Europe*. Budapest: Central European University Press.

Åslund, A., & Snegovaya, M. (2021). The Impact of Western Sanctions on Russia and How They Can Be Made Even More Effective. *Atlantic Council.* Retrieved from https://www.atlanticcouncil.org/in-depth-research-reports/report/the-impact-of-western-sanctions-on-russia/

Asmus, R. D., & Nurick, R. C. (1996). NATO Enlargement and the Baltic States. *Survival, 38*(2), 121-142.

Associated Press. (2017). Хакерська атака уразила до 10% комп'ютерів в Україні, приватних, урядових і комерційних. *VOA News.* Retrieved from https://ukrainian.voanews.com/a/virus-ukraine/3931019.html

Atch, D., & Neray, P. (2017). Operation BugDrop: CyberX Discovers Large-Scale Cyber-Reconnaissance Operation Targeting Ukrainian Organizations. *CyberX.* Retrieved from https://cyberx-labs.com/blog/operation-bugdrop-cyberx-discovers-large-scale-cyber-reconnaissance-operation/

Auchard, E., & Felix, B. (2017). French Candidate Macron Claims Massive Hack as Emails Leaked. *Reuters.* Retrieved from https://www.reuters.com/article/us-france-election-macron-leaks-idUSKBN1812AZ

Aucsmith, D. (2012). Cyberspace is a Domain of War. *War in Cyberspace.* Retrieved from https://cyberbelli.com/2012/05/26/cyberspace-is-a-domain-of-war/

August, O. (2007). The Great Firewall: China's Misguided - and Futile - Attempt to Control What Happens Online. *Wired.* Retrieved from https://www.wired.com/2007/10/ff-chinafirewall/

Aumasson, J.-P. (2017). *Serious Cryptography: A Practical Introduction to Modern Encryption*. San Francisco: No Starch Press.

Axelrod, R., & Iliev, R. (2014). Timing of Cyber Conflict. *Proceedings of the National Academy of Sciences, 111*(4), 1298-1303.

Azzam, I. (1964). The Dispute Between France and Brazil Over Lobster Fishing in the Atlantic. *The International and Comparative Law Quarterly, 13*(4), 1453-1459.

Bain, M. J. (2006). Triangle of Mistrust: Washington, Moscow and Havana. *Journal of Transatlantic Studies, 4*(2), 145-162.

Ball, J. (2016). U.S. Hacked Into Iran's Critical Civilian Infrastructure For Massive Cyberattack, New Film Claims. *BuzzFeed News.* Retrieved from https://www.buzzfeednews.com/article/jamesball/us-hacked-into-irans-critical-civilian-infrastructure-for-ma

Ballerini, F. (2020). Is Brazil's Soft Power Under Threat? *Fair Observer.* Retrieved from https://www.fairobserver.com/region/latin_america/brazil-football-carnival-culture-soft-power-jair-bolsonaro-news-15521/

Balzacq, T., Dombrowski, P., & Reich, S. (2019). Introduction: Comparing Grand Strategies in the Modern World. In T. Balzacq, P. Dombrowski, & S. Reich (Eds.), *Comparative Grand Strategy: A Framework and Cases*. Oxford: Oxford University Press.

Ban, C. (2013). Brazil's Liberal Neo-Developmentalism: New Paradigm or Edited Orthodoxy. *Review of International Political Economy, 20*(2), 298-331.

Banka, A. (2019). The Breakaways: A Retrospective on the Baltic Road to NATO. *War on the Rocks.* Retrieved from https://warontherocks.com/2019/10/the-breakaways-a-retrospective-on-the-baltic-road-to-nato/

Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. *Electronic Frontier Foundation.* Retrieved from https://www.eff.org/cyberspace-independence

Barnes, J. E. (2018). U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections. *The New York Times.* Retrieved from

https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html

Barnes, J. E. (2019). U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say. *The New York Times.* Retrieved from https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html

Barnett, M. N., & Sikkink, K. (2008). From International Relations to Global Society. In C. Reus-Smit & D. Snidal (Eds.), *The Oxford Handbook of International Relations* (pp. 62-83). Oxford: Oxford University Press.

Barrett, B. (2018). Google Chrome Now Labels HTTP Sites as 'Not Secure'. *Wired.* Retrieved from https://www.wired.com/story/google-chrome-https-not-secure-label/

Barzashka, I. (2013). Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme. *The RUSI Journal, 158*(2), 48-56.

Bastos, M. T., & Mercea, D. (2019). The Brexit Botnet and User-Generated Hyperpartisan News. *Social Science Computer Review, 37*(1), 38-54.

BBC. (2012). Russia Internet Blacklist Law Takes Effect. *BBC News.* Retrieved from https://www.bbc.com/news/technology-20096274

BBC. (2016). 18 Revelations from Wikileaks' Hacked Clinton Emails. *BBC News.* Retrieved from https://www.bbc.com/news/world-us-canada-37639370

BBC. (2017). 'Russian Trolls' Promoted California Independence. *BBC News.* Retrieved from https://www.bbc.com/news/blogs-trending-41853131

BBC. (2018). France's Macron Pushes for 'True European Army'. *BBC News.* Retrieved from https://www.bbc.com/news/world-europe-46108633

BBC. (2019). Georgia Hit By Massive Cyber-Attack. *BBC News.* Retrieved from https://www.bbc.com/news/technology-50207192

BBC. (2022). Germany Warns Against Russian Anti-Virus Use. *BBC News.* Retrieved from https://www.bbc.com/news/technology-60738208

Beckley, M. (2015). The Myth of Entangling Alliances: Reassessing the Security Risks of U.S. Defense Pacts. *International Security, 39*(4), 7-48.

Benjamin, D., & Simon, S. (2019). America's Great Satan: The 40-Year Obsession With Iran. *Foreign Affairs, 98*(6), 56-66.

Benkler, Y., Faris, R., & Roberts, H. (2018). *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. New York: Oxford University Press.

Bennett, A. (2004). Case Study Methods: Design, Use, and Comparative Advantages. In D. F. Sprinz & Y. Wolinsky-Nahmias (Eds.), *Models, Numbers, and Cases: Methods for Studying International Relations*. Ann Arbor: University of Michigan Press.

Bennett, A. (2008). Process Tracing: A Bayesian Perspective. In J. M. Box-Steffensmeier, H. E. Brady, & D. Collier (Eds.), *The Oxford Handbook of Political Methodology*. Oxford: Oxford University Press.

Bennett, A., & Elman, C. (2007). Case Study Methods in the International Relations Subfield. *Comparative Political Studies, 40*(2), 170-195.

Bennett, A., Charman, A., & Fairfield, T. (2022). Understanding Bayesianism: Fundamentals for Process Tracers. *Political Analysis*, *30*(2), 298-305.

Bentley, M. (2016). Study: Does Google Have a Political Bias? *Can I Rank?* Retrieved from http://www.canirank.com/blog/analysis-of-political-bias-in-internet-search-engine-results/

Berger, J. (2016). *Contagious: Why Things Catch On*. New York: Simon & Schuster.

Berger, J. (2016). A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case. *The New York Times.* Retrieved from https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html

Berger, J., & Milkman, K. L. (2012). What Makes Online Content Viral? *Journal of Marketing Research, 49*(2), 192-205.

Bergman, R. (2018). When Israel Hatched a Secret Plan to Assassinate Iranian Scientists. *Politico.* Retrieved from https://www.politico.com/magazine/story/2018/03/05/israel-assassination-iranian-scientists-217223

Bergman, R., & Mazzetti, M. (2019). The Secret History of the Push to Strike Iran. *The New York Times.* Retrieved from https://www.nytimes.com/2019/09/04/magazine/iran-strike-israel-america.html

Bessi, A., & Ferrara, E. (2016). Social Bots Distort the 2016 US Presidential Election Online Discussion. *First Monday, 21*(11).

Betts, R. K. (1982). *Surprise Attack: Lessons for Defense Planning*. Washington DC: Brookings Institution.

Betz, D. J. (2012). Cyberpower and International Security. *Foreign Policy Research Institute.* Retrieved from https://www.fpri.org/article/2012/06/cyberpower-and-international-security/

Bevins, V. (2015). Why Did Brazil's President Change Her Tune on Spying? *Foreign Policy.* Retrieved from https://foreignpolicy.com/2015/06/16/brazil-nsa-spying-surveillance-economy-dilma-rousseff-barack-obama/

Bhattacharya, A. (2016). Brazil's "Indefinite" Whatsapp Block Only Lasted Around Four Hours. *Quartz.* Retrieved from https://qz.com/736745/brazils-indefinite-whatsapp-block-only-lasted-around-four-hours/

Biagioli, M., & Lépinay, V. A. (2019). Russian Economies of Codes. In M. Biagioli & V. A. Lépinay (Eds.), *From Russia with Code: Programming Migrations in Post-Soviet Times*. Durham: Duke University Press.

Biddle, S. (2016). Here's the Public Evidence Russia Hacked the DNC - It's Not Enough. *The Intercept.* Retrieved from https://theintercept.com/2016/12/14/heres-the-public-evidence-russia-hacked-the-dnc-its-not-enough/

Biddle, S., Friedman, J. A., & Shapiro, J. N. (2012). Testing the Surge: Why Did Violence Decline in Iraq in 2007? *International Security, 37*(1), 7-40.

Bing, C. (2020). Suspected Russian Hackers Spied on U.S. Treasury Emails - Sources. *Reuters.* Retrieved from https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive/suspected-russian-hackers-spied-on-u-s-treasury-emails-sources-idUKKBN28N0PG

Bing, C., Stubbs, J., & Menn, J. (2019). Exclusive: Western Intelligence Hacked 'Russia's Google' Yandex To Spy On Accounts - Sources. *Reuters.* Retrieved from https://www.reuters.com/article/us-usa-cyber-yandex-exclusive-idUSKCN1TS2SX

Black, J. L. (1999). Russia and NATO Expansion Eastward: Red-Lining the Baltic States. *International Journal, 54*(2), 249-266.

Blainey, G. (1988). *Causes of War* (3rd ed.). New York: The Free Press.

Blake, A. (2016). Here are the Latest, Most Damaging Things in the DNC's Leaked Emails. *The Washington Post.* Retrieved from https://www.washingtonpost.com/news/the-fix/wp/2016/07/24/here-are-the-latest-most-damaging-things-in-the-dncs-leaked-emails

Blinken, A. J. (2022). Attribution of Russia's Malicious Cyber Activity Against Ukraine. *US Department of State.* Retrieved from https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/

Boadle, A. (2014). Brazil To Drop Local Data Storage Rule in Internet Bill. *Reuters.* Retrieved from https://www.reuters.com/article/us-brazil-internet/brazil-to-drop-local-data-storage-rule-in-internet-bill-idUSBREA2I03O20140319

Bode, K. (2020). Russia's War on Encryption Stumbles Forth With Ban of Tutanota. *TechDirt.* Retrieved from https://www.techdirt.com/2020/02/21/russias-war-encryption-stumbles-forth-with-ban-tutanota/

Bogost, I., & Madrigal, A. C. (2020). How Facebook Works for Trump. *The Atlantic.* Retrieved from https://www.theatlantic.com/technology/archive/2020/04/how-facebooks-ad-technology-helps-trump-win/606403/

Bond, S., & Allyn, B. (2022). Russia Is Restricting Social Media. Here's What We Know. *NPR.* Retrieved from https://www.npr.org/2022/03/07/1085025672/russia-social-media-ban

Bordelon, B. (2023). Biden And Congress Want To Ban Tiktok. At This Point It May Be Impossible. *Politico.* Retrieved from https://www.politico.com/news/2023/04/16/why-washington-wont-ban-tiktok-00091690

Borghard, E. D., & Lonergan, S. W. (2017). The Logic of Coercion in Cyberspace. *Security Studies, 26*(3), 452-481.

Borghard, E. D., & Lonergan, S. W. (2018). Why Are There No Cyber Arms Control Agreements? *Council on Foreign Relations.* Retrieved from https://www.cfr.org/blog/why-are-there-no-cyber-arms-control-agreements

Bossert, T. P. (2020). I Was the Homeland Security Adviser to Trump. We're Being Hacked. *The New York Times.* Retrieved from https://www.nytimes.com/2020/12/16/opinion/fireeye-solarwinds-russia-hack.html

Bourantonis, D., & Panagiotou, R. A. (2004). Russia's Attitude Towards the Reform of the United Nations Security Council, 1990-2000. *Journal of Communist Studies and Transition Politics, 20*(4), 79-102.

Bowden, M. (2011). *Worm: The First Digital World War*. New York: Atlantic Monthly Press.

Bown, C. P., & Irwin, D. A. (2019). Trump's Assault on the Global Trading System. *Foreign Affairs.* Retrieved from https://www.foreignaffairs.com/articles/asia/2019-08-12/trumps-assault-global-trading-system

Bradbury, D. (2009). The Fog of Cyberwar. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2009/feb/05/kyrgyzstan-cyberattack-internet-access

Brandom, R. (2016). The Shadow Brokers Hack is Starting to Look Like Russia vs. NSA. *The Verge.* Retrieved from https://www.theverge.com/2016/8/17/12519804/shadow-brokers-russia-nsa-hack-equation-group

Brazil. (2008). National Strategy of Defense. *Ministry of Defense.* Retrieved from https://www2.gwu.edu/~clai/recent_events/2010/Brazil_Defense/National_Strategy_of_Defense.pdf

Brazil. (2012). National Defense White Paper. *Ministry of Defense.* Retrieved from https://www.defesa.gov.br/arquivos/estado_e_defesa/livro_branco/lbdn_2013_ing_net.pdf

Brazil. (2018). Decree No. 9.637, of December 26, 2018. *Executive Branch of the Government of Brazil.* Retrieved from https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/56970098/do1-2018-12-27-decreto-n-9-637-de-26-de-dezembro-de-2018-56969938

Brazil. (2019). Constitution of the Federative Republic of Brazil. *Supreme Federal Court of Brazil.* Retrieved from http://www.stf.jus.br/arquivo/cms/legislacaoConstituicao/anexo/brazil_federal_constitution.pdf

Brennan Center for Justice. (2013). Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs. *Brennan Center for Justice.* Retrieved from https://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf

Bridi, S., & Greenwald, G. (2013). Documentos Revelam Esquema De Agência Dos EUA Para Espionar Dilma. *G1.* Retrieved from http://g1.globo.com/fantastico/noticia/2013/09/documentos-revelam-esquema-de-agencia-dos-eua-para-espionar-dilma-rousseff.html

Brighi, E., & Hill, C. (2016). Implementation and Behaviour. In S. Smith, A. Hadfield, & T. Dunne (Eds.), *Foreign Policy: Theories, Actors, Cases* (3rd ed.). Oxford: Oxford University Press.

Broad, W. J., Markoff, J., & Sanger, D. E. (2011). Israeli Test on Worm Called Crucial in Iran Nuclear Delay. *The New York Times.* Retrieved from https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Broniatowski, D. A., Jamison, A. M., Qi, S., AlKulaib, L., Chen, T., Benton, A., . . . Dredze, M. (2018). Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate. *American Journal of Public Health, 108*(10), 1378-1384.

Brooks, S. G. (1997). Dueling Realisms. *International Organization, 51*(3), 445-477.

Brzezinski, Z. (2013). *Strategic Vision: America and the Crisis of Global Power*. New York: Basic Books.

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

Buchanan, B. (2016). The Life Cycles of Cyber Threats. *Survival, 58*(1), 39-58.

Buchanan, B. (2017a). *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford: Oxford University Press.

Buchanan, B. (2017b). Nobody But Us: The Rise and Fall of the Golden Age of Signals Intelligence. *Belfer Center for Science and International Affairs.* Retrieved from https://www.belfercenter.org/sites/default/files/files/publication/Buchanan%20Nobody%20But%20Us.pdf

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge: Harvard University Press.

Bughin, J., Doogan, J., & Vetvik, O. J. (2010). A New Way to Measure Word-Of-Mouth Marketing. *McKinsey & Company.* Retrieved from https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/a-new-way-to-measure-word-of-mouth-marketing

Burdick, A. (2018). Looking for Life on a Flat Earth. *The New Yorker.* Retrieved from https://www.newyorker.com/science/elements/looking-for-life-on-a-flat-earth

Burgers, T., & Robinson, D. R. S. (2018). Keep Dreaming: Cyber Arms Control is Not a Viable Policy Option. *S&F Sicherheit und Frieden, 36*(3), 140-145.

Burges, S. W. (2008). Consensual Hegemony: Theorizing Brazilian Foreign Policy after the Cold War. *International Relations, 22*(1), 65-84.

Bush, G. W. (2008). Remarks by the President on the Signing of the H.R. 6304, FISA Amendments Act of 2008. *US Department of Justice.* Retrieved from https://www.justice.gov/archive/ll/docs/fisa-amendments-act-2008.pdf

Bussolati, N. (2015). The Rise of Non-State Actors in Cyberwarfare. In J. D. Ohlin, C. Finkelstein, & K. Govern (Eds.), *Cyberwar: Law and Ethics for Virtual Conflicts*. Oxford: Oxford University Press.

Buzan, B. (1991). New Patterns of Global Security in the Twenty-First Century. *International Affairs, 67*(3), 431-451.

Buzan, B., Wæver, O., & Wilde, J. d. (1998). *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers.

Bybee, K. J., & Jenkins, L. (2019). Free Speech, Free Press, and Fake News: What If the Marketplace of Ideas Isn't About Identifying Truth? *Studies in L:aw and Politics, 5*, 95-117.

Bykova, M. F. (2022). Russia and Power: Unmasking the Historical Origins of the Present Crisis. *Studies in East European Thought, 74*(4), 439-446.

Cabestan, J.-P. (2019). China's Military Base in Djibouti: A Microcosm of China's Growing Competition with the United States and New Bipolarity. *Journal of Contemporary China, 29*(125), 1-17.

Callanan, C., Dries-Ziekenheiner, H., Escudero-Pascual, A., & Guerra, R. (2010). Leaping Over the Firewall: A Review of Censorship Circumvention Tools. *Freedom House.* Retrieved from https://freedomhouse.org/sites/default/files/2020-02/Archived_Special_Report_FH_Censorship_Circumvention_tools.pdf

Canabarro, D. R., & Borne, T. (2013). Reflections on the Fog of (Cyber) War. *NCDG Policy Working Paper, 13*(2).

Carr, E. H. (2016). *The Twenty Years' Crisis, 1919-1939*. London: Palgrave Macmillan.

Carr, J. (2013). Mandiant APT1 Report Has Critical Analytic Flaws. *Digital Dao.* Retrieved from http://jeffreycarr.blogspot.com/2013/02/mandiant-apt1-report-has-critical.html

Carvalho, L. (2016). Juiz Manda Bloquear Facebook Em Todo O Brasil Por 24 Horas. *Olhar Digital.* Retrieved from https://olhardigital.com.br/noticia/juiz-manda-bloquear-facebook-em-todo-o-brasil-por-24-horas/62909

Cendrowski, S. (2015). Why China Is Making Life Miserable For Big U.S. Tech. *Fortune.* Retrieved from https://fortune.com/2015/02/26/why-china-is-making-life-miserable-for-big-u-s-tech/

CERT-Georgia. (2011). Cyber Espionage Against Georgian Government (Georbot Botnet). *Ministry of Justice of Georgia.* Retrieved from https://docplayer.net/2643880-Cyber-espionage-against-georgian-government-georbot-botnet-cert-gov-ge-lepl-data-exchange-agency-ministry-of-justice-of-georgia.html

CERT.br. (n.d.). Sobre o CERT.br. *CERT.br.* Retrieved from https://www.cert.br/sobre/

CFR. (2022). Cyber Operations Tracker. *Council on Foreign Relations.* Retrieved from https://www.cfr.org/interactive/cyber-operations

CGI.br. (2014). Marco Civil Law of the Internet in Brazil. *CGI.br.* Retrieved from https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180

CGI.br. (n.d.). Composição do CGI.br. *CGI.br.* Retrieved from https://cgi.br/membros/

Chalfant, M. (2017). State Dept. to Eliminate Cyber Office: Report. *The Hill.* Retrieved from https://thehill.com/policy/cybersecurity/342698-state-dept-to-eliminate-cyber-office-report

Chander, A., & Lê, U. P. (2015). Data Nationalism. *Emory Law Journal, 64*(3), 677-739.

Chatin, M. (2016). Brazil: Analysis of a Rising Soft Power. J*ournal of Political Power, 9*(3), 369-393.

Chen, A. (2015). The Agency. *The New York Times Magazine.* Retrieved from https://www.nytimes.com/2015/06/07/magazine/the-agency.html

Cherepanov, A. (2016). The Rise of TeleBots: Analyzing Disruptive KillDisk Attacks. *We Live Security.* Retrieved from https://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/

Cherepanov, A. (2017). WIN32/INDUSTROYER: A New Threat for Industrial Control Systems. *ESET.* Retrieved from https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

Cherepanov, A., & Lipovsky, R. (2018). New TeleBots Backdoor: First Evidence Linking Industroyer to NotPetya. *WeLiveSecurity.* Retrieved from

https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/

Chernenko, E. (2018). Russia's Cyber Diplomacy. In S. Secrieru & N. Popescu (Eds.), *Hacks, Leaks and Disruptions: Russian Cyber Strategies* (pp. 53-64). Paris: European Union Institute for Security Studies.

Chesney, R. (2020). The CIA, Covert Action and Operations in Cyberspace. *Lawfare.* Retrieved from https://www.lawfareblog.com/cia-covert-action-and-operations-cyberspace

Chhor, K. (2017). As French Media Went Dark, Bbots and Far-Right Activists Drove #MacronLeaks. *France24.* Retrieved from https://www.france24.com/en/20170508-french-media-blackout-bots-far-right-activists-wikileaks-pushed-macronleaks

China, Russian Federation, Tajikistan, & Uzbekistan. (2011). Annex to the Letter Dated 12 September 2011 From the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General *United Nations Digital Library.* Retrieved from https://digitallibrary.un.org/record/710973

Chokshi, N. (2019). Hackers Are Holding Baltimore Hostage: How They Struck and What's Next. *The New York Times.* Retrieved from https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html

Chomsky, N. (1981). Human Rights and American Foreign Policy A Symposium. *Commentary.* Retrieved from https://www.commentarymagazine.com/articles/human-rights-and-american-foreign-policy-a-symposium/

Choucri, N. (2012). *Cyberpolitics in International Relations*. Cambridge: MIT Press.

Choucri, N. (2015). Explorations in Cyber International Relations: A Research Collaboration of MIT and Harvard University. *MIT Political Science Department Research Paper*.

Choucri, N., & Goldsmith, D. (2012). Lost in Cyberspace: Harnessing the Internet, International Relations, and Global Security. *Bulletin of the Atomic Scientists, 68*(2), 70-77.

Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for Cyber Security: International Responses and Global Imperatives. *Information Technology for Development, 20*(2), 96-121.

Cimpanu, C. (2019). Extensive hacking operation discovered in Kazakhstan. *ZDNet.* Retrieved from https://www.zdnet.com/article/extensive-hacking-operation-discovered-in-kazakhstan/

Cimpanu, C. (2020). State-Sponsored Hackers Are Now Using Coronavirus Lures to Infect Their Targets. *ZDNet.* Retrieved from https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/

Clark, D. D. (2018). *Designing an Internet*. Cambridge: MIT Press.

Clark, D. D., & Landau, S. (2011). Untangling Attribution. *Harvard National Security Journal*(2), 323-352.

Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins.

Clarke, R. A., & Knake, R. K. (2019). *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*: Penguin Publishing Group.

Clarke, R. A., Morell, M. J., Stone, G. R., Sunstein, C. R., & Swire, P. (2014). *The NSA Report: Liberty and Security in a Changing World*. Princeton: Princeton University Press.

Cleary, G. (2019). Twitterbots: Anatomy of a Propaganda Campaign. *Symantec Enterprise Blogs/Threat Intelligence.* Retrieved from https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/twitterbots-propaganda-disinformation

Clinton, H. R. (2010). Remarks on Internet Freedom. *US Department of State.* Retrieved from https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

Clinton, H. R. (2011). Internet Rights and Wrongs: Choices & Challenges in a Networked World. *US Department of State.* Retrieved from https://2009-2017.state.gov/secretary/20092013clinton/rm/2011/02/156619.htm

Clinton, H. R. (2017). *What Happened*. New York: Simon & Schuster.

Coase, R. H. (1937). The Nature of the Firm. *Economica, 4*(16), 386-405.

Coase, R. H. (1960). The Problem of Social Cost. *The Journal of Law & Economics, 3*, 1-44.

Cocoradă, E., Maican, C. I., Cazan, A.-M., & Maican, M. A. (2018). Assessing the Smartphone Addiction Risk and its Associations with Personality Traits Among Adolescents. *Children and Youth Services Review, 93*, 345-354.

COE. (2018). Budapest Convention and Related Standards. *Council of Europe.* Retrieved from https://www.coe.int/en/web/cybercrime/the-budapest-convention

Cohen, E. A. (2004). History and the Hyperpower. *Foreign Affairs, 83*(4), 49-63.

Coiera, E. (2000). Information Economics and the Internet. *Journal of the American Medical Informatics Association, 7*(3), 215-221.

Colleoni, E., Rozza, A., & Arvidsson, A. (2014). Echo Chamber or Public Sphere? Predicting Political Orientation and Measuring Political Homophily in Twitter Using Big Data. *Journal of Communication, 64*(2), 317-332.

Cook, J. (2010). 'Cyberation' and Just War Doctrine: A Response to Randall Dipert. *Journal of Military Ethics, 9*(4), 411-423.

Cooper, H. (2016). U.S. Drops Snark in Favor of Emotion to Undercut Extremists. *The New York Times.* Retrieved from https://www.nytimes.com/2016/07/29/world/middleeast/isis-recruiting.html

Cordeiro, L. E. P. C. (2017). Cyber Attacks: Is Brazil Prepared? *Air and Space Power Journal, 29*(2), 4-9.

Cox, R. W. (1981). Social Forces, States and World Orders: Beyond International Relations Theory. *Millennium, 10*(2), 126-155.

Craig, A. J. S., & Valeriano, B. G. (2018). Realism and Cyber Conflict: Security in the Digital Age. In J. R. Avgustin, D. Orsi, & M. Nurnus (Eds.), *Realism in Practice: An Appraisal*. Bristol: E-International Relations.

CRS. (2016). Promoting Global Internet Freedom: Government and Industry Initiatives. *Congressional Research Service.* Retrieved from https://epic.org/crs/R41837.pdf

CrySyS. (2011). Duqu: A Stuxnet-Like Malware Found in the Wild. *Laboratory of Cryptography and System Security.* Retrieved from https://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf

CSIS. (2023). Significant Cyber Incidents. *Center for Strategic and International Studies.* Retrieved from https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

CTIR.Gov. (n.d.). Sobre o CTIR Gov. *CTIR.Gov.* Retrieved from https://www.ctir.gov.br/sobre/

Ctrl+X. (2018). Políticos tentaram ocultar informação mais de 500 vezes durante a campanha. *Abraji.* Retrieved from http://www.ctrlx.org.br/noticia/politicos-tentaram-ocultar-informacao-mais-de-500-vezes-durante-a-campanha

Cull, N. J. (2013). The Long Road to Public Diplomacy 2.0: The Internet in US Public Diplomacy. *International Studies Review, 15*(1), 123-139.

Cunningham, L. (2020). Text of Open Technology Fund update to US Agency for Global Media. *The Washington Post.* Retrieved from https://www.washingtonpost.com/context/text-of-open-technology-fund-update-to-us-agency-for-global-media/92d51e51-616b-4d19-928f-e117a5288c95/?itid=lk_interstitial_manual_23

Curran, J. (2005). What Democracy Requires of the Media. In G. Overholser & K. H. Jamieson (Eds.), *The Institutions of American Democracy: The Press* (pp. 120-137). New York: Oxford University Press.

da Silva, L. I. L. (2009). Lula's Speech at FISL 10, in English. *Software Livre Brasil.* Retrieved from https://softwarelivre.org/portal/fisl/lula-s-speech-at-fisl-10-in-english

da Silva, M. G. (2019). *Cyber Security: A Case Study of Brazil.* (Master of Science in National Security and War Studies). National Defence University, Islamabad. Retrieved from https://bdex.eb.mil.br/jspui/bitstream/123456789/3765/1/CYBER%20SECURITY.pdf

Davis, J. (2007). Hackers Take Down the Most Wired Country in Europe *Wired.* Retrieved from https://www.wired.com/2007/08/ff-estonia/

Dawkins, R. (2016). *The Selfish Gene* (40th Anniversary ed.). Oxford: Oxford University Press.

De Lima, M. R. S., & Hirst, M. (2006). Brazil as an Intermediate State and Regional Power: Action, Choice and Responsibilities. *International Affairs, 82*(1), 21-40.

de Mesquita, B. B., Smith, A., Morrow, J. D., & Siverson, R. M. (2005). *The Logic of Political Survival*. Cambridge: MIT Press.

de Souza Pinheiro, A. (1995). *Guerrilla in The Brazilian Amazon*. Retrieved from Fort Leavenworth: https://community.apan.org/cfs-file/__key/docpreview-s/00-00-08-81-84/1995_2D00_07_2D00_01-Guerrilla-in-the-Brazilian-Amazon-_2800_De-Souza-Pinheiro_2900_.pdf

Deibert, R. J. (2003). Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace. *Millennium, 32*(3), 501-530.

Deibert, R. J., & Rohozinski, R. (2010). Liberation vs. Control: The Future of Cyberspace. *Journal of Democracy, 21*(4), 43-57.

Devanny, J., Goldoni, L. R. F., & Medeiros, B. P. (2022). The Rise of Cyber Power in Brazil. *Revista Brasileira de Política Internacional, 65*(1).

Devetak, R. (1999). Theories, Practices and Postmodernism in International Relations. *Cambridge Review of International Affairs, 12*(2), 61-76.

DeYoung, K., Nakashima, E., & Rauhala, E. (2017). Trump Signed Presidential Directive Ordering Actions to Pressure North Korea. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/trump-signed-presidential-directive-ordering-actions-to-pressure-north-korea/2017/09/30/97c6722a-a620-11e7-b14f-f41773cd5a14_story.html

DHS. (2018). Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. *US Department of Homeland Security.* Retrieved from https://www.us-cert.gov/ncas/alerts/TA18-074A

DHSC. (2018). Securing Cyber Resilience in Health and Care: Progress Update October 2018. *UK Department of Health and Social Care.* Retrieved from https://www.gov.uk/government/publications/securing-cyber-resilience-in-health-and-care-october-2018-update

Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The Second-Generation Onion Router. *Paul Syverson, 13*.

Diniz, G., Glenny, M., & Muggah, R. (2014). Brazil doubles down on cyber security. *openDemocracy.* Retrieved from https://www.opendemocracy.net/en/brazil-doubles-down-on-cyber-security/

Diniz, G., Muggah, R., & Glenny, M. (2014). Deconstructing Cyber Security in Brazil. *Igarapé Institute.* Retrieved from https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf

Dipert, R. R. (2010). The Ethics of Cyberwarfare. *Journal of Military Ethics, 9*(4), 384-410.

DIRCO. (2003). Brasilia Declaration. *SA Department of International Relations and Cooperation.* Retrieved from http://www.dirco.gov.za/docs/2005/ibsa_brasilia.htm

DiResta, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., . . . Johnson, B. (2019). The Tactics & Tropes of the Internet Research Agency. *New Knowledge.* Retrieved from https://digitalcommons.unl.edu/senatedocs/2/

DNI. (2017). Assessing Russian Activities and Intentions in Recent US Elections. *Office of the Director of National Intelligence.* Retrieved from https://www.dni.gov/files/documents/ICA_2017_01.pdf

DNI. (2018). A Guide to Cyber Attribution. *Office of the Director of National Intelligence.* Retrieved from https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf

DOD. (2019). Russian Strategic Intentions: A Strategic Multilayer Assessment (SMA) White Paper. *US Departmenf of Defense.* Retrieved from https://info.publicintelligence.net/SMA-RussianStrategicIntentions.pdf

DOJ. (2018a). Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election. *US Department of Justice,.* Retrieved from https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

DOJ. (2018b). Internet Research Agency Indictment. *US Department of Justice,.* Retrieved from https://www.justice.gov/file/1035477/download

DOJ. (2020). Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace. *US Department of Justice,.* Retrieved from https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

Donaldson, R. H., & Nadkarni, V. (2019). *The Foreign Policy of Russia: Changing Systems, Enduring Interests* (6th ed.): Routledge.

Dorfman, Z., Zetter, K., McLaughlin, J., & Naylor, S. D. (2020). Exclusive: Secret Trump Order Gives CIA More Powers to Launch Cyberattacks. *Yahoo News.* Retrieved from

https://news.yahoo.com/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html

Douglas, K. M., Sutton, R. M., & Cichocka, A. (2017). The Psychology of Conspiracy Theories. *Current Directions in Psychological Science, 26*(6), 538-542.

Douglas, W. O. (1951). Dennis v. United States, 341 U.S. 494. Retrieved from https://www.loc.gov/item/usrep250616/

Doyle, A. C. (1894). *The Memoirs of Sherlock Holmes, Volume II*. Leipzig: Bernhard Tauchnitz.

Dragos. (2018). CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations. *Dragos.* Retrieved from https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf

Drezner, D. W. (2016). Where Have All the Big International Relations Theories Gone? *The Washington Post.* Retrieved from https://www.washingtonpost.com/posteverything/wp/2016/09/14/where-have-all-the-big-international-relations-theories-gone/

Dueck, C., & Takeyh, R. (2007). Iran's Nuclear Challenge. *Political Science Quarterly, 122*(2), 189-205.

Duncan, I. (2019). Ruppersberger: NSA Says 'EternalBlue' Hacking Tool Was Not a Factor in Baltimore Ransomware Attack. *The Baltimore Sun.* Retrieved from https://www.baltimoresun.com/politics/bs-md-ci-eternalblue-ruppersberger-20190531-story.html

Duncan, J. (2014). *The Rise of the Securocrats: The Case of South Africa*. Johannesburg: Jacana Media.

Duncombe, C. (2017). Twitter and Transformative Diplomacy: Social Media and Iran-US Relations. *International Affairs, 93*(3), 545-562.

Dunn Cavelty, M. (2008). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. New York: Routledge.

Dunn Cavelty, M. (2012). *The Militarisation of Cyberspace: Why Less May Be Better.* Paper presented at the 4th International Conference on Cyber Conflict (CyCon).

Dunn Cavelty, M. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics, 20*(3), 701-715.

Dunn Cavelty, M. (2015). The Normalization of Cyber-International Relations. In O. Thränert & M. Zapfe (Eds.), *Strategic Trends 2015* (Vol. 2015, pp. 81-98): ETH Zurich, Center for Security Studies.

Durumeric, Z., Payer, M., Paxson, V., Kasten, J., Adrian, D., Halderman, J., . . . Beekman, J. (2014). *The Matter of Heartbleed*.

Edelman. (2021). 2021 Edelman Trust Barometer. *Edelman.* Retrieved from https://www.edelman.com/sites/g/files/aatuss191/files/2021-01/2021%20Edelman%20Trust%20Barometer_Final.pdf

Edelman. (2022). 2022 Edelman Trust Barometer. *Edelman.* Retrieved from https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022%20Edelman%20Trust%20Barometer%20FINAL_Jan25.pdf

Efrony, D., & Shany, Y. (2018). A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. *American Journal of International Law, 112*(4), 583-657.

Efstathopoulos, C. (2012). Leadership in the WTO: Brazil, India and the Doha Development Agenda. *Cambridge Review of International Affairs, 25*(2), 269-293.

EIU. (2012). Cyber Power Index. *Economist Intelligence Unit.* Retrieved from http://www.cyberhub.com/CyberPowerIndex

Elgin, B., & Riley, M. (2014). Now at the Sands Casino: An Iranian Hacker in Every Server. *Bloomberg Businessweek.* Retrieved from https://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas

EPIC. (2017). Vulnerabilities Equities Process. *Electronic Privacy Information Center.* Retrieved from https://epic.org/privacy/cybersecurity/vep/

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR)relevant Theory? *International Political Science Review, 27*(3), 221-244.

Erthal Abdenur, A., & Frederico Pereira da Silva Gama, C. (2015). Triggering the Norms Cascade: Brazil's Initiatives for Curbing Electronic Espionage. *Global Governance: A Review of Multilateralism and International Organizations, 21*(3), 455-474.

Esfandiari, G. (2010). The Twitter Devolution. *Foreign Policy.* Retrieved from https://foreignpolicy.com/2010/06/08/the-twitter-devolution/

Fan, R., Zhao, J., Chen, Y., & Xu, K. (2014). Anger Is More Influential than Joy: Sentiment Correlation in Weibo. *PLOS One, 9*(10), 1-8.

Fairfield, T., & Charman, A. (2022). *Social Inquiry and Bayesian Inference: Rethinking Qualitative Research*. Cambridge: Cambridge University Press.

Faou, M. (2020). Tracking Turla: New Backdoor Delivered Via Armenian Watering Holes. *We Live Security.* Retrieved from https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/

Farivar, C. (2018). Australia Passes New Law to Thwart Strong Encryption. *Ars Technica.* Retrieved from https://arstechnica.com/tech-policy/2018/12/australia-passes-new-law-to-thwart-strong-encryption/

Farrell, H., & Schneier, B. (2018). Common-Knowledge Attacks on Democracy. *Berkman Klein Center Research Publication*(2018-7).

FBI, CISA, ODNI, & NSA. (2016). Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Cybersecurity and Infrastructure Security Agency (CISA), and the Office of the Director of National Intelligence (ODNI). *Cybersecurity and Infrastructure Security Agency* Retrieved from https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

Fearon, J. D. (1995). Rationalist Explanations for War. *International Organization, 49*(3), 379-414.

Fearon, J. D. (1997). Signaling Foreign Policy Interests: Tying Hands Versus Sinking Costs. *Journal of conflict resolution, 41*(1), 68-90.

Ferguson, Y. H. (1973). The Dominican Intervention of 1965: Recent Interpretations. *International Organization, 27*(4), 517-548.

Fernandes, D. (2017). Condução Coercitiva de Blogueiro é Grave Atentado à Liberdade de Imprensa, diz Repórteres Sem Fronteiras. *BBC News Brasil.* Retrieved from https://www.bbc.com/portuguese/brasil-39309746

Ferreira, J. N. (2014). Building the Marco Civil: A Brief Review of Brazil's Internet Regulation History. In E. R. Biddle, R. Lemos, & M. Price (Eds.), *Stakes are High: Essays on Brazil and the Future of the Global Internet*. Philadelphia: Internet Policy Observatory.

Fidler, D. P. (2017). Requiem for the Internet Freedom Strategy. *Council on Foreign Relations.* Retrieved from https://www.cfr.org/blog/requiem-internet-freedom-strategy

Fifer, J. V. (1966). Bolivia's Boundary with Brazil: A Century of Evolution. *The Geographical Journal, 132*(3), 360-372.

Finley, K. (2016). The Internet Finally Belongs to Everyone. *Wired.* Retrieved from https://www.wired.com/2016/10/internet-finally-belongs-everyone/

Finley, K. (2019a). Australia's Ban on Huawei Is Just More Bad News for China. *Wired.* Retrieved from https://www.wired.com/story/australias-ban-on-huawei-is-just-more-bad-news-for-china/

Finley, K. (2019b). Huawei's Many Troubles: Bans, Alleged Spies, and Backdoors. *Wired.* Retrieved from https://www.wired.com/story/huaweis-many-troubles-bans-alleged-spies-backdoors/

Finn, P. (2007). Cyber Assaults on Estonia Typify a New Battle Tactic. *The Washington Post.* Retrieved from https://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html

Finnemore, M., & Sikkink, K. (1998). International Norm Dynamics and Political Change. *International Organization, 52*(4), 887-917.

FireEye. (2014). APT28: A Window Into Russia's Cyber Espionage Operations? *FireEye.* Retrieved from https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

FireEye. (2016). Spear Phishing Attacks: Why They are Successful and How to Stop Them. *FireEye.* Retrieved from https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf

FireEye. (2019). Advanced Persistent Threat Groups: Who's Who of Cyber Threat Actors. *FireEye.* Retrieved from https://www.fireeye.com/current-threats/apt-groups.html

FireEye. (2020). Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor. *FireEye.* Retrieved from https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Fisher, M. (2014). If Police in Ferguson Treat Journalists Like This, Imagine How They Treat Residents. *Vox.* Retrieved from https://www.vox.com/2014/8/18/6043247/ferguson-police-media-harassment

Fisher, M., & Taub, A. (2019). How YouTube Radicalized Brazil. *The New York Times.* Retrieved from https://www.nytimes.com/2019/08/11/world/americas/youtube-brazil.html

Flemes, D. (2007). Emerging Middle Powers' Soft Balancing Strategy: State and Perspectives of the IBSA Dialogue Forum. *GIGA Working Papers*(57).

Floridi, L., & Taddeo, M. (2014). *The Ethics of Information Warfare*. New York: Springer International Publishing.

FOC. (2023). Slovakia Becomes the 36th Member of the Freedom Online Coalition. *Freedom Online Coalition.* Retrieved from https://freedomonlinecoalition.com/slovakia-becomes-the-36th-member-of-the-freedom-online-coalition/

Ford, C. A. (2010). The Trouble with Cyber Arms Control. *The New Atlantis, Fall 2010*(29), 52-67.

Franceschi-Bicchierai, L. (2016a). Here's the Full Transcript of Our Interview With DNC Hacker 'Guccifer 2.0'. *Vice.* Retrieved from https://www.vice.com/en/article/yp3bbv/dnc-hacker-guccifer-20-full-interview-transcript

Franceschi-Bicchierai, L. (2016b). How Hackers Broke Into John Podesta and Colin Powell's Gmail Accounts. *Vice.* Retrieved from https://www.vice.com/en/article/mg7xjb/how-hackers-broke-into-john-podesta-and-colin-powells-gmail-accounts

Freedom House. (2015). Country Report 2015: Brazil. *Freedom House.* Retrieved from https://freedomhouse.org/report/freedom-net/2015/brazil

Freedom House. (2022). Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet. *Freedom House.* Retrieved from https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet

Frey, R. S., & Al-Roumi, A. (1999). Political Democracy and the Physical Quality of Life: The Cross-National Evidence. *Social Indicators Research, 47*(1), 73-97.

Fried, D., & O'Toole, B. (2019). The New Russia Sanctions Law: What It Does and How to Make It Work. *Atlantic Council.* Retrieved from https://www.atlanticcouncil.org/wp-content/uploads/2017/09/The_New_Russia_Sanctions_Law_web_0929.pdf

Friedman, G. (2008). The Geopolitics of Russia: Permanent Struggle. *Stratfor.* Retrieved from https://worldview.stratfor.com/article/geopolitics-russia-permanent-struggle

Friedman, M. (1953). The Methodology of Positive Economics. In M. Friedman, *Essays in Positive Economics*. Chicago: University of Chicago Press.

Fukuyama, F. (1989). The End of History? *The National Interest*(16), 3-18.

Fukuyama, F. (1996). *Trust: The Social Virtues and the Creation of Prosperity*: Free Press Paperback.

Gabrielle, L. (2020). Briefing on Disinformation and Propaganda Related to COVID-19. *US Department of State.* Retrieved from https://www.state.gov/briefing-with-special-envoy-lea-gabrielle-global-engagement-center-on-disinformation-and-propaganda-related-to-covid-19/

Galeotti, M. (2014). The 'Gerasimov Doctrine' and Russian Non-Linear War. *In Moscow's Shadow.* Retrieved from https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

Galeotti, M. (2016). Putin's Hydra: Inside Russia's Intelligence Services. *European Council on Foreign Relations.* Retrieved from https://ecfr.eu/publication/putins_hydra_inside_russias_intelligence_services/

Galeotti, M. (2019). *We Need to Talk About Putin: How the West Gets Him Wrong*: Random House.

Galeotti, M. (2021). Active Measures: Russia's Covert Global Reach. In G. P. Herd (Ed.), *Russia's Global Reach: A Security and Statecraft Assessment*. Garmisch-Partenkirchen: George C. Marshall European Center for Security Studies.

Gallagher, S. (2014). NSA's Automated Hacking Engine Offers Hands-Free Pwning of the World. *Ars Technica.* Retrieved from https://arstechnica.com/information-technology/2014/03/nsas-automated-hacking-engine-offers-hands-free-pwning-of-the-world/

Gallagher, S. (2017). As US Launches DDoS Attacks, N. Korea Gets More Bandwidth - Fom Russia. *Ars Technica.* Retrieved from https://arstechnica.com/information-technology/2017/10/as-us-launches-ddos-attacks-n-korea-gets-more-bandwidth-from-russia/

Gallagher, S. (2019). Missiles and Drones that Hit Saudi Oil Fields: Made in Iran, but Fired by Whom? *Ars Technica.* Retrieved from https://arstechnica.com/tech-policy/2019/09/missiles-and-drones-that-hit-saudi-oil-fields-made-in-iran-but-fired-by-whom/

Galtung, J. (1996). *Peace by Peaceful Means: Peace and Conflict, Development and Civilization*. Oslo: International Peace Research Institute.

Gamero-Garrido, A. (2014). Cyber Conflicts in International Relations: Framework and Case Studies. *Explorations in Cyber International Relations.* Retrieved from http://content.netmundial.br/files/286.pdf

GAO. (2009). GAO Report to Congressional Committees: U.S. Public Diplomacy: Key Issues for Congressional Oversight. *Government Accountability Office.* Retrieved from https://www.gao.gov/new.items/d09679sp.pdf

Gardini, G. L. (2016). Brazil: What Rise of What Power? *Bulletin of Latin American Research, 35*(1), 5-19.

Gartzke, E. (2013). The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth. *International Security, 38*(2), 41-73.

Gellman, B., & Poitras, L. (2013). U.S., British Intelligence Mining Data From Nine U.S. Internet Companies in Broad Secret Program. *The Washington Post.* Retrieved from https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Gellman, B., & Soltani, A. (2013). NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

Gellman, B., Timberg, C., & Rich, S. (2013). Secret NSA Documents Show Campaign Against Tor Encrypted Network. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/secret-nsa-documents-show-campaign-against-tor-encrypted-network/2013/10/04/610f08b6-2d05-11e3-8ade-a1f23cda135e_story.html

George, A. L., & Bennett, A. (2005). *Case Studies and Theory Development in the Social Sciences*. Cambridge: MIT Press.

Geron, L. (1991). Roads to Baltic Independence. *The World Today, 47*(8/9), 135-138.

Gerovitch, S. (2004). *From Newspeak to Cyberspeak: A History of Soviet Cybernetics*. Cambridge: MIT Press.

Gibson, W. (1984). *Neuromancer*. New York: Ace Books.

Giesea, J. (2015). It's Time to Embrace Memetic Warfare. *Defence Strategic Communications, 1*(1), 67-75.

Giulianotti, R., & Klauser, F. (2012). Sport Mega-Events and 'Terrorism': A Critical Analysis. *International Review for the Sociology of Sport, 47*(3), 307-323.

Glaser, A., Zia, M., Mousavian, H., & von Hippel, F. (2014). Agreeing on Limits for Iran's Centrifuge Program: A Two-Stage Strategy. *Arms Control Today*(44).

Glassman, J. K. (2008). Public Diplomacy 2.0: A New Approach to Global Engagement. *US Department of State.* Retrieved from https://2001-2009.state.gov/r/us/2008/112605.htm

Goble, P. (2019). Will Moscow Open New Military Bases Beyond the Borders of the Former Soviet Union? *The Jamestown Foundation.* Retrieved from https://jamestown.org/program/will-moscow-open-new-military-bases-beyond-the-borders-of-the-former-soviet-union/

Goel, S., Anderson, A., Hofman, J., & Watts, D. J. (2015). The Structural Virality of Online Diffusion. *Management Science, 62*(1), 180-196.

Gold, J. (2019). How Estonia uses Cybersecurity to Strengthen its Position in NATO. *International Centre for Defence and Security.* Retrieved from https://icds.ee/en/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/

Goldsmith, J. (2018). The Failure of Internet Freedom. *The Knight First Amendment Institute.* Retrieved from https://knightcolumbia.org/content/failure-internet-freedom

Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World*. Oxford: Oxford University Press.

Golts, A. (2023). Russia's Military Failures in Ukraine: Causes and Consequences *Stockholm Centre for Eastern European Studies.* Retrieved from https://sceeus.se/en/publications/russias-military-failures-in-ukraine-causes-and-consequences/

Goodin, D. (2013). Puzzle Box: The Quest to Crack the World's Most Mysterious Malware Warhead. *Ars Technica.* Retrieved from https://arstechnica.com/information-technology/2013/03/the-worlds-most-mysterious-potentially-destructive-malware-is-not-stuxnet/

Goodin, D. (2015). How "Omnipotent" Hackers Tied to NSA Hid for 14 Years - and Were Found at last. *Ars Technica.* Retrieved from https://arstechnica.com/information-technology/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/

Goodin, D. (2016). Researchers Crack Open Unusually Advanced Malware that Hid for 5 years. *Ars Technica.* Retrieved from https://arstechnica.com/information-technology/2016/08/researchers-crack-open-unusually-advanced-malware-that-hid-for-5-years/

Goodin, D. (2019). Zeroday Exploit Prices are Higher than Ever, Especially for iOS and Messaging Apps. *Ars Technica.* Retrieved from https://arstechnica.com/information-technology/2019/01/zeroday-exploit-prices-continue-to-soar-especially-for-ios-and-messaging-apps/

Gorman, S. (2007). NSA Program Draws Congress' Ire. *The Baltimore Sun.* Retrieved from https://www.baltimoresun.com/news/bs-xpm-2007-03-28-0703280154-story.html

Gorobets, O. (2016). A Touch of Artistry: Poseidon's APT Boutique. *Kaspersky Lab.* Retrieved from https://www.kaspersky.co.za/blog/poseidon-apt/5165/

Gostev, A. (2012). The Flame: Questions and Answers. *SecureList by Kaspersky.* Retrieved from https://securelist.com/the-flame-questions-and-answers/34344/

Gostev, A. (2014). Agent.btz: a Source of Inspiration? *SecureList by Kaspersky.* Retrieved from https://securelist.com/agent-btz-a-source-of-inspiration/58551/

Götz, E. (2015). It's Geopolitics, Stupid: Explaining Russia's Ukraine Policy. *Global Affairs, 1*(1), 3-10.

Gould, K. A. (2017). Vaccine Safety: Evidence-Based Research Must Prevail. *Dimensions of Critical Care Nursing, 36*(3), 145-147.

Goutam, R. K. (2015). The Problem of Attribution in Cyber Security. *International Journal of Computer Applications, 131*(7), 34-36.

Govil, N., Agrawal, A., & Tippenhauer, N. O. (2017). *On Ladder Logic Bombs in Industrial Control Systems.* Paper presented at the International Workshop on Security and Privacy Requirements Engineering (SECPRE) at the European Symposium on Research in Computer Security (ESORICS).

Graham, T. (2010). The Sources of Russia's Insecurity. *Survival, 52*(1), 55-74.

Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York: Anchor Books.

Greenwald, G. (2013). Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations. *The Guardian.* Retrieved from https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books.

Greenwald, G., Demori, L., & Reed, B. (2019). How and Why the Intercept Is Reporting on a Vast Trove of Materials about Brazil's Operation Car Wash and Justice Minister Sergio Moro. *The Intercept.* Retrieved from https://theintercept.com/2019/06/09/brazil-archive-operation-car-wash/

Greenwald, G., Kaz, R., & Casado, J. (2013). EUA Espionaram Milhões de E-mails e Ligações de Brasileiros. *O Globo.* Retrieved from https://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934

Griffiths, J. L. (2017). *Cyber Security as an Emerging Challenge to South African National Security.* (Master of Security Studies). University of Pretoria, Retrieved from https://repository.up.ac.za/bitstream/handle/2263/62639/Griffiths_Cyber_2017.pdf

Grigsby, A. (2014). UN Committee Adopts Resolution on Right to Privacy in the Digital Age. *Council on Foreign Relations.* Retrieved from https://www.cfr.org/blog/un-committee-adopts-resolution-right-privacy-digital-age

Grimes, R. A. (2019). Are Zero-Day Exploits the New Norm? *CSO.* Retrieved from https://www.csoonline.com/article/3341393/are-zero-day-exploits-the-new-norm.html

Grix, J., Brannagan, P. M., & Houlihan, B. (2015). Interrogating States' Soft Power Strategies: A Case Study of Sports Mega-Events in Brazil and the UK. *Global Society, 29*(3), 463-479.

Grix, J., Brannagan, P. M., & Lee, D. (2019). *Entering the Global Arena: Emerging States, Soft Power Strategies and Sports Mega-Events*. Singapore: Palgrave Macmillan.

Gruber, L. (2000). *Ruling the World: Power Politics and the Rise of Supranational Institutions*. Princeton: Princeton University Press.

GSI. (2020). Decreto No 10.222, de 5 de Fevereiro de 2020: Aprova a Estratégia Nacional de Segurança Cibernética. *Diário Oficial da União.* Retrieved from https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm

Guitton, C. (2013). Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK? *European Security, 22*(1), 21-35.

Gutterman, S. (2014). Russia Blocks Internet Sites of Putin Critics. *Reuters.* Retrieved from https://www.reuters.com/article/cnews-us-russia-internet-idCABREA2C21L20140313

Gvosdev, N. K. (2014). Ukraine's Ancient Hatreds. *The National Interest*(132), 16-24.

Gvosdev, N. K. (2019). Is Russia Sabotaging Democracy in the West? *Orbis, 63*(3), 321-333.

Haag, M., & Salam, M. (2017). Gunman in 'Pizzagate' Shooting Is Sentenced to 4 Years in Prison. *The New York Times.* Retrieved from https://www.nytimes.com/2017/06/22/us/pizzagate-attack-sentence.html

Haberman, M., & Conger, K. (2020). Trump Prepares Order to Limit Social Media Companies' Protections. *The New York Times.* Retrieved from https://www.nytimes.com/2020/05/28/us/politics/trump-executive-order-social-media.html

Hamburger, T., & Tumulty, K. (2016). WikiLeaks Releases Thousands of Documents About Clinton and Internal Deliberations. *The Washington Post.* Retrieved from https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/

Handel, M. I. (1984). Intelligence and the Problem of Strategic Surprise. *Journal of Strategic Studies, 7*(3), 229-281.

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly, 53*(4), 1155-1175.

Haoran, S., & Yusha, Z. (2019). Most Cyber Attacks From the US: Report. *Global Times.* Retrieved from https://www.globaltimes.cn/content/1153777.shtml

Harding, L. (2019). Yevgeny Prigozhin: Who is the Man Leading Russia's Push into Africa? *The Guardian.* Retrieved from https://www.theguardian.com/world/2019/jun/11/yevgeny-prigozhin-who-is-the-man-leading-russias-push-into-africa

Hare, P. (2020). Public Diplomacy and Soft Power? No Thanks, It's America First. *USC Center on Public Diplomacy.* Retrieved from https://uscpublicdiplomacy.org/blog/public-diplomacy-and-soft-power-no-thanks-its-america-first

Harris, S., & Hudson, J. (2013). Not Even the NSA Can Crack the State Dept's Favorite Anonymous Network. *Foreign Policy.* Retrieved from https://foreignpolicy.com/2013/10/04/not-even-the-nsa-can-crack-the-state-depts-favorite-anonymous-network/

Hayden, M. V. (2011). The Future of Things "Cyber". *Strategic Studies Quarterly, Spring 2011*, 3-7.

Hayden, M. V. (2016). The making of America's cyberweapons. *The Christian Science Monitor.* Retrieved from https://www.csmonitor.com/World/Passcode/Passcode-Voices/2016/0224/The-making-of-America-s-cyberweapons

Haynes, T. (2018). Dopamine, Smartphones & You: A Battle For Your Time. *Science in the News.* Retrieved from http://sitn.hms.harvard.edu/flash/2018/dopamine-smartphones-battle-time/

Healey, J. (2013). *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Washington DC: Cyber Conflict Studies Association.

Healey, J. (2016). The US Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers. *Journal of International Affairs*, 1-22.

Heath, E. (1969). Realism in British Foreign Policy. *Foreign Affairs, 48*(1), 39-50.

Hern, A. (2017). WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

Hernandez, S. (2018). Russian Trolls Spread Baseless Conspiracy Theories Like Pizzagate And QAnon After The Election. *Buzzfeed News.* Retrieved from https://www.buzzfeednews.com/article/salvadorhernandez/russian-trolls-spread-baseless-conspiracy-theories-like

Herrick, D. (2016, 31 May-3 June 2016). *The Social Side of 'Cyber Power'? Social Media and Cyber Operations.* Paper presented at the 8th International Conference on Cyber Conflict (CyCon).

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks Digital Threats and Multinational Responses. *Journal of Strategic Security, 4*(2), 49-60.

Hestres, L. E., & Hopke, J. E. (2017, 2017-09-26). Internet-Enabled Activism and Climate Change. *Oxford Research Encyclopedia of Climate Science.* Retrieved from https://oxfordre.com/climatescience/view/10.1093/acrefore/9780190228620.001.0001/acrefore-9780190228620-e-404

Hickey, M. (2017). The NSA Exploits Are Works of Art, Robust, Reliable, Anti-forensics, Network IDS Evasion Techniques, Static Binaries for Run-Time. *Twitter.* Retrieved from https://twitter.com/hackerfantastic/status/851558488560074752

Hill, J. F. (2012). A U.N. Takeover of the Internet: Existential Threat or Tempest in a Teapot? *Belfer Center for Science and International Affairs.* Retrieved from https://www.belfercenter.org/publication/un-takeover-internet-existential-threat-or-tempest-teapot

Himelboim, I., McCreery, S., & Smith, M. (2013). Birds of a Feather Tweet Together: Integrating Network and Content Analyses to Examine Cross-Ideology Exposure on Twitter. *Journal of Computer-Mediated Communication, 18*(2), 40-60.

Ho, M. Y. (2017). Implications of Near-Autarky for North Korean Economy. *Journal of Economic Theory and Econometrics, 28*(2), 112-134.

Holbrooke, R. (2001). Get the Message Out. *The Washington post.* Retrieved from https://www.washingtonpost.com/archive/opinions/2001/10/28/get-the-message-out/b298b3c9-45b8-45e2-9ec7-20503dd38802/

Hollis, D. (2011). Cyberwar Case Study: Georgia 2008. *Small Wars Journal.* Retrieved from https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008

Holmes, O. W. (1919). Abrams v. United States, 250 U.S. 616. *US Supreme Court.* Retrieved from https://www.loc.gov/item/usrep250616/

Holsti, K. J. (1998). The Problem of Change in International Relations Theory *Institute of International Relations: The University of British Columbia*(Working Paper No. 26), 1-21.

Hopewell, K. (2015). Different Paths to Power: The Rise of Brazil, India and China at the World Trade Organization. *Review of International Political Economy, 22*(2), 311-338.

Hosking, G. A. (1997). *Russia: People and Empire, 1552-1917*. Cambridge: Harvard University Press.

Howard, P. N., Ganesh, B., Liotsiou, D., Kelly, J., & François, C. (2019). The IRA, Social Media and Political Polarization in the United States, 2012-2018. *University of Oxford & Graphika.* Retrieved from https://digitalcommons.unl.edu/senatedocs/1/

HRW. (2014). United States Landmine Policy: Questions and Answers. *Human Rights Watch.* Retrieved from https://www.hrw.org/news/2014/10/03/united-states-landmine-policy-questions-and-answers

Hudson, J. (2017). No Deal: How Secret Talks With Russia To Prevent Election Meddling Collapsed. *Buzzfeed News.* Retrieved from https://www.buzzfeednews.com/article/johnhudson/no-deal-how-secret-talks-with-russia-to-prevent-election

Hulcoop, A., Scott-Railton, J., Tanchak, P., Brooks, M., & Deibert, R. (2016). Tainted Leaks: Disinformation and Phishing With a Russian Nexus. *Citizen Lab.* Retrieved from https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/

Hundley, A. C. (2017). Fake News and the First Amendment: How False Political Speech Kills the Marketplace of Ideas Comments. *Tulane Law Review, 92*(2), 497-518.

Huntington, S. P. (1993). The Clash of Civilizations? *Foreign Affairs, 72*(3), 22-49.

Hurd, I. (2008). Constructivism. In C. Reus-Smit & D. Snidal (Eds.), *The Oxford Handbook of International Relations* (pp. 41-61). Oxford: Oxford University Press.

Hurel, L. M. (2020). Brazil's First National Cybersecurity Strategy: An Analysis of its Past, Present and Future. *School of Public Policy at the Georgia Institute of Technology.* Retrieved from https://www.internetgovernance.org/2020/04/05/brazils-first-national-cybersecurity-strategy-an-analysis-of-its-past-present-and-future

Hurel, L. M., & Lobato, L. C. (2018). A Strategy for Cybersecurity Governance in Brazil. *Igarapé Institute.* Retrieved from https://igarape.org.br/wp-content/uploads/2019/01/A-Strategy-for-Cybersecurity-Governance-in-Brazil.pdf

ICANN. (2015). Multistakeholder Model. *Internet Corporation for Assigned Names and Numbers.* Retrieved from https://icannwiki.org/Multistakeholder_Model

Ikenberry, G. J. (2011). *Liberal Leviathan: The Origins, Crisis, and Transformation of the American World Order*. Princeton: Princeton University Press.

Ingber, S. (1984). The Marketplace of Ideas: A Legitimizing Myth. *Duke Law Journal, 1984*(1), 1-91.

Interfax-Ukraine. (2018). SBU Thwarts Cyber Attack Fom Russia Against Chlorine Station in Dnipropetrovsk Region. *Interfax-Ukraine.* Retrieved from https://en.interfax.com.ua/news/general/517337.html

International Crisis Group. (2018). The Iran Nuclear Deal at Two: A Status Report. *International Crisis Group.* Retrieved from https://www.crisisgroup.org/middle-east-north-africa/gulf-and-arabian-peninsula/iran/181-iran-nuclear-deal-two-status-report

Interpol. (2014). INTERPOL Brings Together Sporting Event Security Experts to Exchange Best Practices. *International Criminal Police Organization.* Retrieved from https://www.interpol.int/en/News-and-Events/News/2014/INTERPOL-brings-together-sporting-event-security-experts-to-exchange-best-practices

ITU. (2009). Overview of Cybersecurity. Recommendation ITU-T X.1205. *International Telecommunication Union.* Retrieved from https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items

Ivanov, A. (2016). ExPetr/Petya/NotPetya is a Wiper, Not Ransomware. *SecureList by Kaspersky.* Retrieved from https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/

Iyengar, S., Lelkes, Y., Levendusky, M., Malhotra, N., & Westwood, S. J. (2019). The Origins and Consequences of Affective Polarization in the United States. *Annual Review of Political Science, 22*(1), 129-146.

Jamieson, K. H. (2018). *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know*. New York: Oxford University Press.

Jarnow, J. (2018). The Ghost of John Perry Barlow Lives in His Posthumous Memoir. *Wired.* Retrieved from https://www.wired.com/story/the-ghost-of-john-perry-barlow-lives-in-his-posthumous-memoir/

Jefferson, T. (2006). First Inaugural Address. *The Papers of Thomas Jefferson.* Retrieved from https://jeffersonpapers.princeton.edu/selected-documents/first-inaugural-address-0

Jensen, B. M., Valeriano, B. G., & Maness, R. C. (2016). *Cyber Compellence: Applying Coercion in the Information Age.* Paper presented at the Annual Meeting of the International Studies Association (ISA).

Jensen, B. M., Valeriano, B. G., & Maness, R. C. (2019). Fancy Bears and Digital Trolls: Cyber Strategy With a Russian Twist. *Journal of Strategic Studies, 42*(2), 212-234.

Jervis, R. (1978). Cooperation under the Security Dilemma. *World Politics, 30*(2), 167-214.

Jervis, R. (2003). Understanding the Bush Doctrine. *Political Science Quarterly, 118*(3), 365-388.

Johnson, A. L. (2016). Strider: Cyberespionage Group Turns Eye of Sauron on Targets *Symantec.* Retrieved from https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ce2df4da-afe9-4a24-b28c-0fb3ba671d95

Johnson, C. (2010). *Dismantling the Empire: America's Last Best Hope*. New York: Metropolitan Books.

Jones, I., & Roy, P. (2021). Sputnik V COVID-19 Vaccine Candidate Appears Safe and Effective. *The Lancet, 397*(10275), 642-643.

Jones, R. L. (2018). Can You Have Too Much of a Good Thing: The Modern Marketplace of Ideas Symposium: Truth, Trust and the First Amendment in the Digital Age. *Missouri Law Review*(4), 971-988.

Joo, T. W. (2014). The Worst Test of Truth: The Marketplace of Ideas as Faulty Metaphor. *Tulane Law Review*(2), 383-434.

Jordan, W., & Radhakrishnan, R. (2015). 'Ex-Israeli Agents' Threatened Cyber Attack on S Africa. *Al Jazeera.* Retrieved from https://www.aljazeera.com/news/2015/02/agents-threatened-cyber-attack-africa-150224153915523.html

Jorion, P. (2000). Risk Management Lessons from Long-Term Capital Management. *European Financial Management, 6*(3), 277-300.

Joyce, R. (2017). Improving and Making the Vulnerability Equities Process Transparent is the Right Thing to Do. *The White House.* Retrieved from https://www.whitehouse.gov/articles/improving-making-vulnerability-equities-process-transparent-right-thing/

Kacowicz , A. M. (2004). Case Study Methods in International Security Studies. In D. F. Sprinz & Y. Wolinsky-Nahmias (Eds.), *Models, Numbers, and Cases: Methods for Studying International Relations*. Ann Arbor: University of Michigan Press.

Kahn, H. (2017). *On Thermonuclear War*. New York: Routledge.

Kahn, T. (2010). Internet Freedom and the Challenge of a Principled Foreign Policy. *SAIS Review of International Affairs, 30*(2), 17-19.

Kaiser, K. (1971). Transnational Politics: Toward a Theory of Multinational Politics. *International Organization, 25*(4), 790-817.

Kal, R. (2016). Governing the Internet. *The American Journal of International Law, 110*(3), 491-503.

Kaplan, F. (2017). *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster.

Kaplan, T. (2019). How the Trump Campaign Used Facebook Ads to Amplify His 'Invasion' Claim. *The New York Times.* Retrieved from https://www.nytimes.com/2019/08/05/us/politics/trump-campaign-facebook-ads-invasion.html

Karagiannis, E. (2013). The 2008 Russian-Georgian War Via the Lens of Offensive Realism. *European Security, 22*(1), 74-93.

Kaspersky. (2014). The Regin Platform: Nation-State Ownage of GSM Networks. *Kaspersky Lab.* Retrieved from https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08070305/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf

Kaspersky. (2015a). Equation Group: Questions and Answers. *Kaspersky Lab.* Retrieved from https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf

Kaspersky. (2015b). Equation: The Death Star of Malware Galaxy. *SecureList by Kaspersky.* Retrieved from https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/

Kaspersky. (2016). Poseidon Group: a Targeted Attack Boutique specializing in global cyber-espionage. *SecureList by Kaspersky.* Retrieved from https://securelist.com/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/73673/

Kaspersky. (2019). APT Trends Report Q1 2019. *SecureList by Kaspersky.* Retrieved from https://securelist.com/apt-trends-report-q1-2019/90643/

Kaspersky, E. (2017). StoneDrill: We've Found New Powerful 'Shamoon-ish' Wiper Malware - and It's Serious. *Kaspersky Lab.* Retrieved from https://eugene.kaspersky.com/2017/03/06/stonedrill-weve-found-new-powerful-shamoon-ish-wiper-malware-and-its-serious/

Katz, R. (2014). The State Department's Twitter War With ISIS Is Embarrassing. *Time.* Retrieved from https://time.com/3387065/isis-twitter-war-state-department/

Katz, Y. (2010). 'Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years'. *The Jerusalem Post.* Retrieved from https://www.jpost.com/iranian-threat/news/stuxnet-virus-set-back-irans-nuclear-program-by-2-years

Kaufmann, C. (2004). Threat Inflation and the Failure of the Marketplace of Ideas: The Selling of the Iraq War. *International Security, 29*(1), 5-48.

Kean, T., & Hamilton, L. H. (2011). *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Authorized Edition ed.). New York: W. W. Norton & Company.

Keegan, J. (2004). *Intelligence In War: Knowledge of the Enemy from Napoleon to Al-Qaeda*. London: Pimlico.

Kegley, C. W. (1993). The Neoidealist Moment in International Studies? Realist Myths and the New International Realities: ISA Presidential Address March 27, 1993 Acapulco, Mexico. *International Studies Quarterly, 37*(2), 131-146.

Kehl, D., Bankston, K., Greene, R., & Morgus, R. (2014). Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity. *Open Technology Institute.* Retrieved from https://newamerica.org/documents/947/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity.pdf

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security, 38*(2), 7-40.

Kello, L. (2014). The Virtual Weapon: Dilemmas and Future Scenarios. [Les cyberarmes : dilemmes et futurs possibles]. *Politique Étrangère, Winter Issue*(4), 139-150.

Kello, L. (2017). *The Virtual Weapon and International Order*. New Haven: Yale University Press.

Kenna Security. (2015). The Remediation Gap: Why Companies Are Losing the Battle Against Non-Targeted Attacks. *Kenna Security.* Retrieved from http://pages.kennasecurity.com/rs/958-PRK-049/images/Kenna-NonTargetedAttacksReport.pdf

Kennan, G. F. (1946). The Long Telegram. *Truman Library.* Retrieved from https://www.trumanlibrary.gov/library/research-files/telegram-george-kennan-james-byrnes-long-telegram

Kennedy, P. (1989). *The Rise and Fall of the Great Powers: Economic Change and Military Conflict From 1500 to 2000*. New York: Vintage Books.

Keohane, R. O. (1982). The Demand for International Regimes. *International Organization, 36*(2), 325-355.

Keohane, R. O. (1984). *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton: Princeton University Press.

Keohane, R. O., & Nye, J. S. (1973). Power and Interdependence. *Survival, 15*(4), 158-165.

Keohane, R. O., & Nye, J. S. (1998). Power and Interdependence in the Information Age. *Foreign Affairs, 77*(5), 81-94.

Keohane, R. O., & Victor, D. G. (2016). Cooperation and Discord in Global Climate Policy. *Nature Climate Change, 6*(6), 570-575.

Kessler, G. (2023). The Hunter Biden Laptop and Claims of 'Russian Disinfo'. *The Washington Post.* Retrieved from https://www.washingtonpost.com/politics/2023/02/13/hunter-biden-laptop-claims-russian-disinfo/

Khan, M. (2017). Companies Face High Cost to Meet New EU Data Protection Rules. *Financial Times.* Retrieved from https://www.ft.com/content/0d47ffe4-ccb6-11e7-b781-794ce08b24dc

Kindleberger, C. P. (1973). *The World in Depression 1929-1939*. Berkeley: University of California Press.

Kindleberger, C. P. (1981). Dominance and Leadership in the International Economy: Exploitation, Public Goods, and Free Rides. *International Studies Quarterly, 25*(2), 242-254.

King, G., Keohane, R. O., & Verba, S. (1994). *Designing Social Inquiry: Scientific Inference in Qualitative Research*. Princeton: Princeton University Press.

Kissinger, H. A. (2014). To Settle the Ukraine Crisis, Start at the End. *The Washington Post.* Retrieved from https://www.washingtonpost.com/opinions/henry-kissinger-to-settle-the-ukraine-crisis-start-at-the-end/2014/03/05/46dad868-a496-11e3-8466-d34c451760b9_story.html

Klimburg, A. (2017). *The Darkening Web: The War for Cyberspace*. New York: Penguin Books.

Knowlton, B. (2007). Nuclear-Armed Iran Risks 'World War III,' Bush Says. *The New York Times.* Retrieved from https://www.nytimes.com/2007/10/17/world/americas/17iht-prexy.4.7932027.html

Koebler, J. (2016). 'Guccifer 2.0' Claims Responsibility for DNC Hack, Releases Docs to Prove it. *Vice.* Retrieved from https://www.vice.com/en/article/3davvy/guccifer-20-claims-responsibility-for-dnc-hack-releases-documents

Koppel, T. (2015). *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath*. New York: Crown Publishers.

Korns, S. W., & Kastenberg, J. E. (2009). Georgia's Cyber Left Hook. *US Army War College.* Retrieved from https://apps.dtic.mil/sti/pdfs/ADA636632.pdf

Kostadinov, D. (2013). Estonia: To Black Out an Entire Country - Part One. *InfoSec Institute.* Retrieved from https://resources.infosecinstitute.com/topic/estonia-to-black-out-an-entire-country-part-one/

Kostyuk, N., & Gartzke, E. (2022). Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine. *Texas National Security Review, 5*(3), 113-126.

Kotkin, S. (2016). Russia's Perpetual Geopolitics: Putin Returns to the Historical Pattern. *Foreign Affairs, 95*(3), 2-9.

Koval, N. (2015). Revolution Hacking. In K. Geers (Ed.), *Cyber War in Perspective: Russian Aggression Against Ukraine*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence Publications.

Kramer, A. E., & Perlroth, N. (2012). Expert Issues a Cyberwar Warning. *The New York Times.* Retrieved from https://www.nytimes.com/2012/06/04/technology/cyberweapon-warning-from-kaspersky-a-computer-security-expert.html

Krasner, S. D. (1976). State Power and the Structure of International Trade. *World Politics, 28*(3), 317-347.

Krasner, S. D. (1978). *Defending the National Interest: Raw Materials Investments and U.S. Foreign Policy*. Princeton: Princeton University Press.

Krasner, S. D. (1982). Structural Causes and Regime Consequences: Regimes as Intervening Variables. *International Organization, 36*(2), 185-205.

Krasner, S. D. (1985). *Structural Conflict: The Third World Against Global Liberalism*. Berkeley: University of California Press.

Krasner, S. D. (1991). Global Communications and National Power: Life on the Pareto Frontier. *World Politics, 43*(3), 336-366.

Kratochwil, F. V. (1989). *Rules, Norms, and Decisions: On the Conditions of Practical and Legal Reasoning in International Relations and Domestic Affairs*. Cambridge: Cambridge University Press.

Kravchenko, S., Al Ali, N., & Khrennikov, I. (2017). This $5 Billion Encrypted App Isn't for Sale at Any Price. *Bloomberg.* Retrieved from https://www.bloomberg.com/news/articles/2017-12-12/cryptic-russian-crusader-says-his-5-billion-app-can-t-be-bought

Kravets, D. (2008). Protect America Act Debate: Truth or Fear Mongering? *Wired.* Retrieved from https://www.wired.com/2008/02/protect-ameri-1/

Krebs, B. (2017). Blowing the Whistle on Bad Attribution. *Krebs on Security.* Retrieved from https://krebsonsecurity.com/2017/08/blowing-the-whistle-on-bad-attribution/

Krebs, B. (2020). VMware Flaw a Vector in SolarWinds Breach? *Krebs on Security.* Retrieved from https://krebsonsecurity.com/2020/12/vmware-flaw-a-vector-in-solarwinds-breach/

Kremez, V. (2020). Pro-Russian CyberSpy Gamaredon Intensifies Ukrainian Security Targeting. *Sentinel Labs.* Retrieved from https://labs.sentinelone.com/pro-russian-cyberspy-gamaredon-intensifies-ukrainian-security-targeting/

Kurowska, X. (2020). What Does Russia Want in Cyber Diplomacy? In D. Broeders & B. van den Berg (Eds.), *Governing Cyberspace: Behavior, Power and Diplomacy* (pp. 105-126). London: Rowman & Littlefield.

Kuzmenko, O., & Cobus, P. (2017). Cyber Firm Rewrites Part of Disputed Russian Hacking Report. *VOA News.* Retrieved from https://www.voanews.com/usa/cyber-firm-rewrites-part-disputed-russian-hacking-report

Lake, D. A. (2006). American Hegemony and the Future of East-West Relations. *International Studies Perspectives, 7*(1), 23-30.

Lake, D. A. (2008). The State and International Relations. In C. Reus-Smit & D. Snidal (Eds.), *The Oxford Handbook of International Relations* (pp. 41-61). Oxford: Oxford University Press.

Lam, O. (2019). Chinese Authorities Go After Citizens for Using VPNs, Skirting Online Censorship. *Global Voices Advox.* Retrieved from https://advox.globalvoices.org/2019/01/11/chinese-authorities-go-after-citizens-for-using-vpns-skirting-online-censorship/

Langner, R. (2013). *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. The Langner Group. Retrieved from https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Langø, H.-I. G. (2013). Slaying Cyber Dragons: Competing Academic Approaches to Cyber Security. *Norwegian Institute of International Affairs.* Retrieved from https://nupi.brage.unit.no/nupi-xmlui/handle/11250/277537

Lantian, A., Muller, D., Nurra, C., & Douglas, K. M. (2017). "I Know Things They Don't Know!": The Role of Need for Uniqueness in Belief in Conspiracy Theories. *Social Psychology, 48*(3), 160-173.

Larrabee, F. S. (2010). Russia, Ukraine, and Central Europe: The Return of Geopolitics. *Journal of International Affairs, 63*(2), 33-52.

Lawson, S. T. (2013). Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. *Journal of Information Technology & Politics, 10*(1), 86-103.

Lawson, S. T., Yeo, S. K., Yu, H., & Greene, E. (2016). *The Cyber-Doom Effect: The Impact of Fear Appeals in the US Cyber Security Debate.* Paper presented at the 8th International Conference on Cyber Conflict (CyCon).

Leach, P. (2018). Nuclear Stability-Cyber Instability: A New Look at an Old Cold War Theory. *Small Wars Journal.* Retrieved from https://smallwarsjournal.com/jrnl/art/nuclear-stability-cyber-instability-new-look-old-cold-war-theory

Lebow, R. N. (1994). The Long Peace, the End of the Cold War, and the Failure of Realism. *International Organization, 48*(2), 249-277.

Lecher, C., & Brandom, R. (2019). Is Huawei a Security Threat? Seven Experts Weigh In. *The Verge.* Retrieved from https://www.theverge.com/2019/3/17/18264283/huawei-security-threat-experts-china-spying-5g

Lee, K.-F. (2018). *AI Superpowers: China, Silicon Valley, and the New World Order*. Boston: Houghton Mifflin Harcourt.

Lee, R. M., Assante, M. J., & Conway, T. (2016a). Analysis of the Cyber Attack on the Ukrainian Power Grid. *Electricity Information Sharing and Analysis Center.* Retrieved from https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Lee, R. M., Assante, M. J., & Conway, T. (2016b). Analysis of the Recent Reports of Attacks on US Infrastructure by Iranian Actors. *SANS ICS Security.* Retrieved from https://ics.sans.org/media/SANSICS_DUC4_Analysis_of_Attacks_on_US_Infrastructure_V1.1.pdf

Lee, T. B. (2012). Authoritarian Regimes Push for Larger ITU Role in DNS System. *Ars Technica.* Retrieved from https://arstechnica.com/tech-policy/2012/12/authoritarian-regimes-push-for-larger-itu-role-in-dns-system/

Lee, T. B. (2013a). Here's Everything We Know About PRISM to Date. *The Washington Post.* Retrieved from https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/

Lee, T. B. (2013b). How Congress Unknowingly Legalized PRISM in 2007. *The Washington Post.* Retrieved from https://www.washingtonpost.com/news/wonk/wp/2013/06/06/how-congress-unknowingly-legalized-prism-in-2007/

Leetaru, K. H. (2015). A Few Good Twitter Trolls. *Foreign Policy.* Retrieved from https://foreignpolicy.com/2015/07/14/islamic-state-twitter-recruiting/

Lemos, R. (2007). Artigo: Internet Brasileira Precisa de Marco Regulatório Civil. *UOL Noticias.* Retrieved from https://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm

Lesaca, J. (2017). Why Did Russian Social Media Swarm the Digital Conversation about Catalan Independence? *The Washington Post.* Retrieved from https://www.washingtonpost.com/news/monkey-cage/wp/2017/11/22/why-did-russian-social-media-swarm-the-digital-conversation-about-catalan-independence/

Lessig, L. (1999). *Code and Other Laws of Cyberspace*. New York: Basic Books.

Levine, Y. (2018). *Surveillance Valley: The Secret Military History of the Internet*. New York: PublicAffairs.

Levy, S. (2014). How the NSA Almost Killed the Internet. *Wired.* Retrieved from https://www.wired.com/2014/01/how-the-us-almost-killed-the-internet/

Lewis, J. (2017). Is the United States Really Blowing Up North Korea's Missiles? *Foreign Policy.* Retrieved from https://foreignpolicy.com/2017/04/19/the-united-states-isnt-hacking-north-koreas-missile-launches/

Lewis, J. A. (2016). The US Really Does Want to Constrain Commercial Espionage: Why Does Nobody Believe It? *Center for Strategic and International Studies.* Retrieved from https://www.csis.org/blogs/strategic-technologies-blog/us-really-does-want-constrain-commercial-espionage-why-does-nobody

Lewis, J. A. (2018). ZTE, the Telecom Wars, and Cyber Spies. *Center for Strategic and International Studies.* Retrieved from https://www.csis.org/analysis/zte-telecom-wars-and-cyber-spies

Lewis, M. (2018). Has Anyone Seen the President? *Bloomberg News.* Retrieved from https://www.bloomberg.com/opinion/articles/2018-02-09/has-anyone-seen-the-president

Leyden, J. (2017). Watership Downtime: BadRabbit Encrypts Russian Media, Ukraine Transport Hub PCs. *The Register.* Retrieved from https://www.theregister.com/2017/10/24/badrabbit_ransomware/

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation.

Libicki, M. C., Ablon, L., & Webb, T. (2015). *The Defender's Dilemma: Charting a Course Toward Cybersecurity*. Santa Monica: RAND Corporation.

Lichtenstein, J. (2010). Digital Diplomacy. *The New York Times Magazine.* Retrieved from https://www.nytimes.com/2010/07/18/magazine/18web2-0-t.html

Lieber, K. A., & Alexander, G. (2005). Waiting for Balancing: Why the World Is Not Pushing Back. *International Security, 30*(1), 109-139.

Lilly, B., & Cheravitch, J. (2017). *The Past, Present, and Future of Russia's Cyber Strategy and Forces*. Paper presented at the 12th International Conference on Cyber Conflict (CyCon).

Limberg, P. N., & Barnes, C. (2018). The Memetic Tribes Of Culture War 2.0. *Intellectual Explorers.* Retrieved from https://medium.com/s/world-wide-wtf/memetic-tribes-and-culture-war-2-0-14705c43f6bb

Lindsay, J. M. (2011). George W. Bush, Barack Obama and the Future of US Global Leadership. *International Affairs, 87*(4), 765-779.

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies, 22*(3), 365-404.

Lindsay, J. R., & Gartzke, E. (2018). Coercion Through Cyberspace: The Stability-Instability Paradox Revisited. In K. M. Greenhill & P. Krause (Eds.), *Coercion: The Power to Hurt in International Politics*: Oxford University Press.

Lipton, E., Sanger, D. E., & Shane, S. (2016). The Perfect Weapon: How Russian Cyberpower Invaded the U.S. *The New York Times.* Retrieved from https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

Lobato, L. C., & Kenkel, K. M. (2015). Discourses of Cyberspace Securitization in Brazil and in the United States. *Revista Brasileira de Política Internacional, 58*(2), 23-43.

Londoño, E., & Casado, L. (2020). Glenn Greenwald Charged With Cybercrimes in Brazil. *The New York Times.* Retrieved from https://www.nytimes.com/2020/01/21/world/americas/glenn-greenwald-brazil-cybercrimes.html

Lonsdale, D. (1999). Information Power: Strategy, Geopolitics, and the Fifth Dimension. In C. S. Gray & G. Sloan (Eds.), *Geopolitics, Geography and Strategy* (pp. 137-157). London: Frank Cass Publishers.

LRT.lt. (2020). Lithuania Came Under Biggest Cyber Attack in Years, Says Defence Minister. *LRT English.* Retrieved from https://www.lrt.lt/en/news-in-english/19/1300455/lithuania-came-under-biggest-cyber-attack-in-years-says-defence-minister

Lustig, R. (2010). Brazil Emerges as a Leading Exponent of 'Soft Power'. *BBC News.* Retrieved from http://news.bbc.co.uk/2/hi/americas/8580560.stm

Luttwak, E. N. (1979). *The Grand Strategy of the Roman Empire: From the First Century A.D. to the Third*. Baltimore: Johns Hopkins University Press.

Luttwak, E. N. (2009). *The Grand Strategy of the Byzantine Empire*. Cambridge: Belknap Press.

Lynch, C., & Gramer, R. (2020). Pompeo Aims to Cut Funds for Program Honoring Envoy Killed in Benghazi. *Foreign Policy.* Retrieved from https://foreignpolicy.com/2020/02/14/pompeo-trump-administration-benghazi-public-diplomacy-state-department-christopher-stevens-federal-budget/

Lynn III, W. J. (2010). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs, 89*(5), 97-108.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique. *Big Data & Society, 1*(2), 1-13.

MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013). GCHQ Taps Fibre-Optic Cables for Ssecret Access to World's Communications. *The Guardian.* Retrieved from https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

Mackey, R. (2016). What Julian Assange's War on Hillary Clinton Says About WikiLeaks. *The Intercept.* Retrieved from https://theintercept.com/2016/08/06/accusing-wikileaks-bias-beside-point/

MacKinnon, R., Wilson, A., & Woolery, L. (2016). Internet Freedom at a Crossroads: Recommendations for the 45th President's Internet Freedom Agenda. *New America.* Retrieved from https://www.newamerica.org/documents/1736/Internet__Freedom_Agenda_12_21.pdf

Malamud, A. (2011). A Leader Without Followers? The Growing Divergence Between the Regional and Global Performance of Brazilian Foreign Policy. *Latin American Politics and Society, 53*(3), 1-24.

Malamud, A., & Alcañiz, I. (2017). Managing Security in a Zone of Peace: Brazil´s Soft Approach to Regional Governance. *Revista Brasileira de Política Internacional, 60*(1).

Malinoswki, T. (2015). The Leading Internet Freedom Technology (LIFT) Initiative: Scaling Up U.S. Leadership to Promote Human Rights Online. *US Department of State.* Retrieved from http://2007-2017-blogs.state.gov/stories/2015/10/12/leading-internet-freedom-technology-lift-initiative-scaling-us-leadership-promote.html

Malle, S. (2013). Economic Modernisation and Diversification in Russia. Constraints and Challenges. *Journal of Eurasian Studies, 4*(1), 78-99.

Mallick, P. K. (2022). Decoding Russia's 'Missing' Cyberwar Amid War in Ukraine. *Vivekananda International Foundation.* Retrieved from https://www.vifindia.org/sites/default/files/Decoding-Russia-s-Missing-Cyberwar-Amid-War-in-Ukraine.pdf

Mandiant. (2013). APT1: Exposing One of China's Cyber Espionage Units. *Mandiant.* Retrieved from https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Mandiant. (2020). 'Ghostwriter' Influence Campaign: Unknown Actors Leverage Website Compromises and Fabricated Content to Push Narratives Aligned with Russian Security Interests. *Mandiant.* Retrieved from https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/Ghostwriter-Influence-Campaign.pdf

Manjikian, M. M. (2010). From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly, 54*(2), 381-401.

Maras, M.-H. (2010). How to Catch a Terrorist: Is Mass Surveillance the Answer? *Journal of Applied Security Research, 5*(1), 20-41.

Marczak, B., Alexander, G., McKune, S., Scott-Railton, J., & Deibert, R. (2017). Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware. *Citizen Lab.* Retrieved from https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/

Markoff, J. (2009). Vast Spy System Loots Computers in 103 Countries. *The New York Times.* Retrieved from https://www.nytimes.com/2009/03/29/technology/29spy.html

Markoff, J., & Kramer, A. E. (2009). U.S. and Russia Differ on a Treaty for Cyberspace. *The New York Times.* Retrieved from https://www.nytimes.com/2009/06/28/world/28cyber.html

Marks, J. (2011). Agency Uses Circumvention Tools to Advance Democracy. *NextGov.* Retrieved from https://www.nextgov.com/technology-news/2011/08/agency-uses-circumvention-tools-to-advance-democracy/49648/

Marten, K. (2015). Putin's Choices: Explaining Russian Foreign Policy and Intervention in Ukraine. *The Washington Quarterly, 38*(2), 189-204.

Martin, D. (2016). Russian Hack Almost Brought the U.S. Military to Its Knees. *CBS News.* Retrieved from https://www.cbsnews.com/news/russian-hack-almost-brought-the-u-s-military-to-its-knees/

Martin, R. (2016). In Fight Against ISIS, U.S. Adds Cyber Tools. *NPR.* Retrieved from https://www.npr.org/transcripts/468446138

Martinez-Bravo, M., & Stegmann, A. (2019). In Vaccines We Trust? The Effects of the CIA's Vaccine Ruse on Immunization in Pakistan. *Center for Monetary and Financial Studies.* Retrieved from https://www.cemfi.es/~martinez-bravo/mmb/Research_files/MS_Vaccines.pdf

Matos, M. M. d. (2020). The Unclassical Match Between Brazil and Argentina: Past and Present of the Nuclear-Weapon-Free Zone in Latin America and the Caribbean. In J. L. Black-Branch & D. Fleck (Eds.), *Nuclear Non-Proliferation in International Law* (Vol. V, pp. 151-168). The Hague: T.M.C. Asser Press.

Matthews, M., Migacheva, K., & Brown, R. A. (2021). Superspreaders of Malign and Subversive Information on COVID-19: Russian and Chinese Efforts Targeting the United States. *RAND Corporation.* Retrieved from https://www.rand.org/pubs/research_reports/RRA112-11.html

Maurer, T., & Morgus, R. (2014). Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate. *Internet Governance Papers.* Retrieved from https://d1y8sb8igg2f8e.cloudfront.net/documents/no7_2.pdf

McAdams, A. J. (2005). Internet Surveillance after September 11: Is the United States Becoming Great Britain? *Comparative Politics, 37*(4), 479-498.

McCarthy, T. (2017). How Russia Used Social Media to Divide Americans. *The Guardian.* Retrieved from https://www.theguardian.com/us-news/2017/oct/14/russia-us-politics-social-media-facebook

McFaul, M. (2020). Putin, Putinism, and the Domestic Determinants of Russian Foreign Policy. *International Security, 45*(2), 95-139.

McGuire, M. (2018). Into The Web of Profit. *Bromium.* Retrieved from https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf

McLaughlin, J., Dorfman, Z., & Naylor, S. D. (2019). Pentagon Secretly Struck Back Against Iranian Cyberspies Targeting U.S. Ships. *Yahoo News.* Retrieved from https://news.yahoo.com/pentagon-secretly-struck-back-against-iranian-cyber-spies-targeting-us-ships-234520824.html

McPherson, M., Smith-Lovin, L., & Cook, J. M. (2001). Birds of a Feather: Homophily in Social Networks. *Annual Review of Sociology, 27*(1), 415-444.

Mearsheimer, J. J. (1990). Back to the Future: Instability in Europe After the Cold War. *International Security, 15*(1), 5-56.

Mearsheimer, J. J. (1994). The False Promise of International Institutions. *International Security, 19*(3), 5-49.

Mearsheimer, J. J. (2003). *The Tragedy of Great Power Politics* (2nd ed.). New York: W. W. Norton & Company.

Mearsheimer, J. J. (2014). Why the Ukraine Crisis Is the West's Fault: The Liberal Delusions That Provoked Putin. *Foreign Affairs, 93*(5), 77-89.

Mearsheimer, J. J. (2018). *Great Delusion: Liberal Dreams and International Realities*. New Haven: Yale University Press.

Mearsheimer, J. J., & Walt, S. M. (2013). Leaving Theory Behind: Why Simplistic Hypothesis Testing is Bad for International Relations. *European Journal of International Relations*, 19(3), 427–457.

Medeiros, F. A., & Bygrave, L. A. (2015). Brazil's Marco Civil da Internet: Does It Live Up to the Hype? *Computer Law & Security Review, 31*(1), 120-130.

Menn, J. (2013). Exclusive: Secret Contract Tied NSA and Security Industry Pioneer. *Reuters.* Retrieved from https://www.reuters.com/article/us-usa-security-rsa/exclusive-secret-contract-tied-nsa-and-security-industry-pioneer-idUSBRE9BJ1C220131220

Meyer, D. (2014). Brazilian Lawmakers Approve Bill of Online Rights, Minus Local Storage Requirements. *Gigaom.* Retrieved from https://gigaom.com/2014/03/26/brazilian-lawmakers-approve-bill-of-online-rights-minus-local-storage-requirements/

Meyers, A. (2016). Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units. *CrowdStrike Blog.* Retrieved from https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/

Mihov, D. (2017). DailyMotion Suffers the Wrath of Russia With Permanent Ban Nationwide. *TNW.* Retrieved from https://thenextweb.com/news/dailymotion-russia-permanent-ban

Milani, C. R. S., & Nery, T. (2019). Brazil: Political Bot Intervention During Pivotal Events. In T. Balzacq, P. Dombrowski, & S. Reich (Eds.), *Comparative Grand Strategy: A Framework and Cases*. Oxford: Oxford University Press.

Mill, J. S. (2017). *On Liberty and the Subjection of Women*. Seattle: AmazonClassics.

Miller, C. (2020). A Viral Email About Coronavirus Had People Smashing Buses And Blocking Hospitals. *BuzzFeed News.* Retrieved from https://www.buzzfeednews.com/article/christopherm51/coronavirus-ukraine-china

Miller, G. (2020). 'The Intelligence Coup of the Century'. *The Washington Post.* Retrieved from https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

Miller, G., & Higham, S. (2015). In a Propaganda War Against ISIS, the U.S. Tried to Play by the Enemy's Rules. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/in-a-propaganda-war-us-tried-to-play-by-the-enemys-rules/2015/05/08/6eb6b732-e52f-11e4-81ea-0649268f729e_story.html

Mills, R. A. (2018). Pop-Up Political Advocacy Communities on Reddit.com: SandersForPresident and The Donald. *AI & Society, 33*(1), 39-54.

Milton, J. (1918). *Areopagitica, with a Commentary by Sir Richard C. Jebb and with Supplementary Material* (R. Jebb Ed.). Cambridge: Cambridge University Press.

Mitchell, C. R. (1989). *The Structure of International Conflict*. London: Palgrave Macmillan.

Mitrovic, Z., & Thakur, C. (2019). *Positioning South Africa in the BRICS Cybersecurity Context: A Strategic Perspective*. Paper presented at the International Conference on Cyber Warfare and Security (ICCWS).

Modderkolk, H. (2018). Dutch Agencies Provide Crucial Intel About Russia's Interference in US-Elections. *de Volkskrant.* Retrieved from https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/

Modena, C. (2012). Governo Destina Baixo Orçamento Para a Segurança Cibernética. *G1.* Retrieved from http://g1.globo.com/jornal-da-globo/noticia/2013/07/governo-destina-baixo-orcamento-para-seguranca-cibernetica.html

Molla, R., & Stewart, E. (2019). Should Social Media Companies be Legally Responsible for Misinformation and Hate Speech? 2020 Democrats Weigh In. *Vox.* Retrieved from https://www.vox.com/policy-and-politics/2019/12/3/20965459/tech-2020-candidate-policies-section230-facebook-misinformation-hate-speech

Moltke, H. (2019). Mission Creep: How the NSA's Game-Changing Targeting System Built for Iraq and Afghanistan Ended Up on the Mexico Border. *The Intercept.* Retrieved from https://theintercept.com/2019/05/29/nsa-data-afghanistan-iraq-mexico-border/

Moore, T., Friedman, A., & Procaccia, A. D. (2010). *Would a 'Cyber Warrior' Protect Us? Exploring Trade-Offs Between Attack and Defense of Information Systems*. Paper presented at the New Security Paradigms Workshop (NPSW).

Morgenthau, H. J. (1949). The Primacy of the National Interest. *The American Scholar, 18*(2), 207-212.

Morgenthau, H. J. (1993). *Politics Among Nations: The Struggle for Power and Peace* (6th ed.). New York: McGraw-Hill.

Morozov, E. (2009a). The Future of "Public Diplomacy 2.0". *Foreign Policy.* Retrieved from https://foreignpolicy.com/2009/06/09/the-future-of-public-diplomacy-2-0/

Morozov, E. (2009b). Iran: Downside to the "Twitter Revolution". *Dissent, 56*, 10-14.

Mostrous, A., Bridge, M., & Gibbons, K. (2017). Russia Used Twitter Bbots and Trolls 'To Disrupt' Brexit Vote. *The Times.* Retrieved from https://www.thetimes.co.uk/article/russia-used-web-posts-to-disrupt-brexit-vote-h9nv5zg6c

Motyl, A. J. (2015). The Surrealism of Realism: Misreading the War in Ukraine. *World Affairs, 177*(5), 75-84.

Mueller, R. S. (2019). Report on the Investigation into Russian Interference in the 2016 Presidential Election. *US Department of Justice,.* Retrieved from https://www.justice.gov/storage/report.pdf

Muggah, R., & Thompson, N. B. (2017). Brazil Struggles With Effective Cyber-Crime Response. *Jane's Intelligence Review.* Retrieved from https://www.janes.com/images/assets/518/73518/Brazil_struggles_with_effective_cyber-crime_response.pdf

Mulligan, D. K., & Bamberger, K. A. (2018). Saving Governance-By-Design. *California Law Review, 106*(3), 697-784.

Muncaster, P. (2018). Five Eyes Nations United in Blaming Russia for NotPetya. *Infosecurity Magazine.* Retrieved from https://www.infosecurity-magazine.com/news/five-eyes-united-blaming-russia/

Myers, S. L. (2007). Russia Rebukes Estonia for Moving Soviet Statue. *The New York Times.* Retrieved from https://www.nytimes.com/2007/04/27/world/europe/27cnd-estonia.html

Nagle, A. (2017). *Kill All Normies: Online Culture Wars From 4Chan And Tumblr To Trump And The Alt-Right*. Alresford: John Hunt Publishing.

Najibullah, F. (2014). Russian TV Announces Right Sector Leader Led Ukraine *Radio Free Europe/Radio Liberty.* Retrieved from https://www.rferl.org/a/russian-tv-announces-right-sector-leader-yarosh-led-ukraine-polls/25398882.html

Nakashima, E. (2017a). New Details Emerge About 2014 Russian Hack of the State Department: It Was 'Hand to Hand Combat'. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/new-details-emerge-about-2014-russian-hack-of-the-state-department-it-was-hand-to-hand-combat/2017/04/03/d89168e0-124c-11e7-833c-503e1f6394c9_story.html

Nakashima, E. (2017b). NSA Employee Who Worked on Hacking Tools at Home Pleads Guilty to Spy Charge. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/nsa-employee-who-worked-on-hacking-tools-at-home-pleads-guilty-to-spy-charge/2017/12/01/ec4d6738-d6d9-11e7-b62d-d9345ced896d_story.html

Nakashima, E. (2018). Russian Military Was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

Nakashima, E. (2019). U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html

Nakashima, E. (2022). Russian Military Behind Hack of Satellite Communication Devices in Ukraine at War's Outset, U.S. Officials Say. *The Washington Post.* Retrieved from https://www.washingtonpost.com/national-security/2022/03/24/russian-military-behind-hack-satellite-communication-devices-ukraine-wars-outset-us-officials-say/

Nakashima, E., & Harris, S. (2020). Elite CIA Unit That Developed Hacking Tools Failed to Secure Its Own Systems, Allowing Massive Leak, an Internal Report Found. *The Washington Post.* Retrieved from https://www.washingtonpost.com/national-security/elite-cia-unit-that-developed-hacking-tools-failed-to-secure-its-own-systems-allowing-massive-leak-an-internal-report-found/2020/06/15/502e3456-ae9d-11ea-8f56-63f38c990077_story.html

Nakashima, E., Miller, G., & Tate, J. (2012). U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html

Nakashima, E., & Rucker, P. (2017). U.S. Declares North Korea Carried Out Massive Wannacry Cyberattack. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html

Nakashima, E., & Warrick, J. (2010). Stuxnet Was Work of U.S. and Israeli Experts, Officials Say. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

Nakashima, E., & Warrick, J. (2013). For NSA Chief, Terrorist Threat Drives Passion to 'Collect It All'. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html

Napoli, P. M. (2018). What If More Speech Is No Longer the Solution: First Amendment Theory Meets Fake News and the Filter Bubble. *Federal Communications Law Journal, 70*(1), 55-104.

Narula, S. (2004). Psychological Operations (PSYOPs): A Conceptual Overview. *Strategic Analysis, 28*(1), 177-192.

NATO. (1995). Study on NATO Enlargement. *North Atlantic Treaty Organization.* Retrieved from https://www.nato.int/cps/en/natohq/official_texts_24733.htm

NATO. (2014). Wales Summit Declaration. *North Atlantic Treaty Organization.* Retrieved from https://www.nato.int/cps/en/natohq/official_texts_112964.htm

Nazario, J. (2009). Politically Motivated Denial of Service Attacks. In C. Czosseck & K. Geersa (Eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare* (pp. 163-181). Amsterdam: IOS Press.

NCCIC, & FBI. (2016). GRIZZLY STEPPE – Russian Malicious Cyber Activity. *National Cybersecurity and Communications Integration Center & Federal Bureau of Investigation.* Retrieved from https://us-cert.cisa.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

NCSC. (2018). Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed. *National Cyber Security Centre.* Retrieved from https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed

Negus, S. (2006). Victory in Iraq Impossible, Says Kissinger. *Financial Times.* Retrieved from https://www.ft.com/content/c2daddb2-7822-11db-be09-0000779e2340

Nemer, D. (2016). Online Favela: The Use of Social Media by the Marginalized in Brazil. *Information Technology for Development, 22*(3), 364-379.

Newman, L. H. (2018). The Leaked NSA Spy Tool That Hacked the World. *Wired.* Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

NIC.br. (n.d.). Sobre o NIC.br. *NIC.br.* Retrieved from https://nic.br/sobre/

Nielsen. (2015). Global Trust in Advertising. *The Nielsen Company.* Retrieved from https://www.nielsen.com/wp-content/uploads/sites/3/2019/04/global-trust-in-advertising-report-sept-2015-1.pdf

Nimmo, B. (2017). #ElectionWatch: Scottish Vote, Pro-Kremlin Trolls. *Medium.* Retrieved from https://medium.com/dfrlab/electionwatch-scottish-vote-pro-kremlin-trolls-f3cca45045bb

Nisbet, E. (2015). Benchmarking Public Demand: Russia's Appetite for Internet Control. *Center for Global Communication Studies.* Retrieved from http://globalnetpolicy.org/wp-content/uploads/2015/02/Russia-Public-Opinion.pdf

Nissenbaum, H. (2005). Where Computer Security Meets National Security. *Ethics and Information Technology, 7*(2), 61-73.

North, D. C. (1991). Institutions. *Journal of Economic Perspectives, 5*(1), 97-112.

NSA. (2015). Discovering IT Problems, Developing Solutions, Sharing Expertise. *National Security Agency.* Retrieved from https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/1625787/infographic-discovering-it-problems-developing-solutions-sharing-expertise/

Nye, J. S. (1990). Soft Power. *Foreign Policy, 80*(Autumn, 1990), 153-171.

Nye, J. S. (2010). Cyber Power. *Belfer Center for Science and International Affairs.* Retrieved from https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf

Nye, J. S. (2011a). *The Future of Power*. New York: PublicAffairs.

Nye, J. S. (2011b). Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly, (Winter): 18–38*.

Nye, J. S. (2015). *Is the American Century Over?* Hoboken: John Wiley & Sons.

Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security, 41*(3), 44-71.

Nye, J. S., & Keohane, R. O. (1971a). Transnational Relations and World Politics: A Conclusion. *International Organization, 25*(3), 721-748.

Nye, J. S., & Keohane, R. O. (1971b). Transnational Relations and World Politics: An Introduction. *International Organization, 25*(3), 329-349.

O'Brien, D. (2018). In the New Fight for Online Privacy and Security, Australia Falls: What Happens Next? *Electronic Frontier Foundation.* Retrieved from https://www.eff.org/deeplinks/2018/12/new-fight-online-privacy-and-security-australia-falls-what-happens-next

O'Maley, D. (2016). How Brazil Crowdsourced a Landmark Law. *Foreign Policy.* Retrieved from https://foreignpolicy.com/2016/01/19/how-brazil-crowdsourced-a-landmark-law/

O'Neill, P. H. (2017a). Leaked NSA Tools, Now Infecting Over 200,000 Machines, Will Be Weaponized For Years. *CyberScoop.* Retrieved from https://www.cyberscoop.com/leaked-nsa-tools-now-infecting-over-200000-machines-will-be-weaponized-for-years/

O'Neill, P. H. (2017b). Researchers Link Macron Hack to APT28 With 'Moderate Confidence'. *CyberScoop.* Retrieved from https://www.cyberscoop.com/researchers-link-macron-hack-to-apt28-with-moderate-confidence/

Obama, B. H. (2013). Obama Takes Questions on NSA Surveillance Program. *The Wall Street Journal.* Retrieved from https://www.wsj.com/video/obama-takes-questions-on-nsa-surveillance-program/BD300672-8E68-432B-B61A-097598B6713B.html

Odell, J. S. (2004). Case Study Methods in International Political Economy. In D. F. Sprinz & Y. Wolinsky-Nahmias (Eds.), *Models, Numbers, and Cases: Methods for Studying International Relations*. Ann Arbor: University of Michigan Press.

Olson, M. (1965). *The Logic of Collective Action: Public Goods and the Theory of Groups*. Cambridge: Harvard University Press.

Onuf, N. G. (1989). *World of Our Making: Rules and Rule in Social Theory and International Relations*. Columbia: University of South Carolina Press.

Orenstein, M. A., & Schmitz, H. P. (2006). The New Transnationalism and Comparative Politics. *Comparative Politics, 38*(4), 479-500.

Osnos, E., Remnick, D., & Yaffa, J. (2017). Trump, Putin, and the New Cold War. *The New Yorker.* Retrieved from https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war

Ottis, R. (2008). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. Paper presented at the 7th European Conference on Information Warfare (ECCWS).

Page, S. (1994). The Creation of a Sphere of Influence: Russia and Central Asia. *International Journal, 49*(4), 788-813.

Parker, A. (2017). Trump Claims to Be Victim Of 'Witch Hunt' Following Appointment of Special Counsel in Russia Case. *The Washington Post.* Retrieved from https://www.washingtonpost.com/news/post-politics/wp/2017/05/18/trump-claims-to-be-victim-of-witch-hunt-following-appointment-of-special-counsel-in-russia-case/

Parliament. (1848). Treaty of Adrianople: Charges Against Viscount Palmerston. *UK Parliament.* Retrieved from https://hansard.parliament.uk/commons/1848-03-01/debates/2221a5d7-

21f5-49c5-a64a-cc333b61d517/TreatyOfAdrianople%E2%80%94ChargesAgainstViscountPalmerston

Parliament. (2020). Russia. *Intelligence and Security Committee of the UK Parliament.* Retrieved from https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf

Pasko, M. T. (2000). Re-Defining National Security in the Technology Age: The Encryption Export Debate Note. *Journal of Legislation, 26*(2), 337-354.

Paul, C., & Matthews, M. (2016). The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It. *RAND Corporation.* Retrieved from https://www.rand.org/pubs/perspectives/PE198.html

Pauw, J. (2017). *The President's Keepers: Those Keeping Zuma in Power and Out of Prison*. Cape Town: Tafelberg.

PBS NewsHour. (2014). How Should the U.S. Government Respond to North Korea's Attack On Sony. *PBS.* Retrieved from https://www.pbs.org/newshour/show/u-s-government-respond-north-koreas-attack-sony

Pedro, T. (2016). Brazil's Cyberspace Politics: Combining Emerging Threats With Old Intentions. *Politikon, 29*(2016), 295-309.

Perlroth, N. (2012). In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. *The New York Times.* Retrieved from https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

Perlroth, N., & Hardy, Q. (2013). Bank Hacking Was the Work of Iranians, Officials Say. *The New York Times.* Retrieved from https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html

Perlroth, N., Larson, J., & Shane, S. (2013). N.S.A. Able to Foil Basic Safeguards of Privacy on Web. *The New York Times.* Retrieved from https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html

Perlroth, N., & Rosenberg, M. (2020). Russians Hacked Ukrainian Gas Company at Center of Impeachment. *The New York Times.* Retrieved from https://www.nytimes.com/2020/01/13/us/politics/russian-hackers-burisma-ukraine.htmlRussians

Perlroth, N., & Sanger, D. E. (2014). North Korea Loses Its Link to the Internet. *The New York Times.* Retrieved from https://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html

Perlroth, N., & Shane, S. (2019). In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc. *The New York Times.* Retrieved from https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html

Pernik, P. (2018). The Early Days of Cyberattacks: The Cases of Estonia, Georgia and Ukraine. In S. Secrieru & N. Popescu (Eds.), *Hacks, Leaks and Disruptions: Russian Cyber Strategies* (pp. 53-64). Paris: European Union Institute for Security Studies.

Peters, B. (2016). *How Not to Network a Nation: The Uneasy History of the Soviet Internet*. Cambridge: MIT Press.

Pettyjohn, S. L., & Wasser, B. (2019). Competing in the Gray Zone. *RAND Corporation.* Retrieved from https://www.rand.org/pubs/research_reports/RR2791.html

Pew. (2017). Share of Democrats Calling Russia 'Greatest Danger' To U.S. Is At Its Highest Since End of Cold War. *Pew Research Center.* Retrieved from https://www.pewresearch.org/fact-tank/2017/04/20/share-of-democrats-calling-russia-greatest-danger-to-u-s-at-its-highest-since-end-of-cold-war/

Pew. (2019). Bipartisan Support for Increased U.S. Sanctions against Russia. *Pew Research Center.* Retrieved from https://www.pewresearch.org/politics/2014/04/28/bipartisan-support-for-increased-u-s-sanctions-against-russia/

Pleming, S. (2009). U.S. State Department Speaks to Twitter Over Iran. *Reuters.* Retrieved from https://www.reuters.com/article/us-iran-election-twitter-usa-idUSWBT01137420090616

Polyakova, A. (2018). Trump Has Trapped Himself Into Cracking Down On Russia. *Brookings Institution.* Retrieved from https://www.brookings.edu/blog/order-from-chaos/2018/09/25/on-the-record-the-u-s-administrations-actions-on-russia/

Polyakova, A., & Letsas, F. (2019). On The Record: The U.S. Administration's Actions on Russia. *Brookings Institution.* Retrieved from https://www.brookings.edu/blog/order-from-chaos/2018/09/25/on-the-record-the-u-s-administrations-actions-on-russia/

Pomerantsev, P. (2014). Russia and the Menace of Unreality. *The Atlantic.* Retrieved from https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/

Pomerantsev, P. (2017). *Nothing is True and Everything is Possible: Adventures in Modern Russia*. London: Faber & Faber.

Pomerantsev, P. (2019). *This Is Not Propaganda: Adventures in the War Against Reality*. London: Faber & Faber.

Pompeo, M. R. (2018). Remarks by Secretary Pompeo at the German Marshall Fund. *US Department of State.* Retrieved from https://ua.usembassy.gov/remarks-by-secretary-pompeo-at-the-german-marshall-fund/

Porter, M. E. (1996). What is Strategy? *Harvard Business Review, November-December 1996*.

Poulsen, K. (2014). Apple's iPhone Encryption Is a Godsend, Even if Cops Hate It. *Wired.* Retrieved from https://www.wired.com/2014/10/golden-key/

Price, B. C. (2012). Targeting Top Terrorists: How Leadership Decapitation Contributes to Counterterrorism. *International Security, 36*(4), 9-46.

Prokop, A. (2018). 23 Tweets From @TEN_GOP, One Russian-Run Twitter Account Mentioned in Mueller's New Indictment. *Vox.* Retrieved from https://www.vox.com/policy-and-politics/2017/10/19/16504510/ten-gop-twitter-russia

Proofpoint. (2018). The Human Factor 2018. *Proofpoint.* Retrieved from https://www.proofpoint.com/sites/default/files/pfpt-uk-tr-the-human-factor-2018.pdf

Prosser, M. B. (2006). *Memetics - A Growth Industry in US Military Operations.* (Master of Operational Studies). United States Marine Corps School of Advanced Warfighting, Retrieved from https://apps.dtic.mil/sti/pdfs/ADA507172.pdf

Putin, V. (2007). Speech and the Following Discussion at the Munich Conference on Security Policy. *The Kremlin.* Retrieved from http://en.kremlin.ru/events/president/transcripts/24034

Putin, V. (2014). Full Text of Putin's Speech on Crimea. *Prague Post.* Retrieved from https://www.praguepost.com/eu-news/37854-full-text-of-putin-s-speech-on-crimea

Putin, V. (2018). A Plea for Caution From Russia. *The New York Times.* Retrieved from https://www.nytimes.com/2013/09/12/opinion/putin-plea-for-caution-from-russia-on-syria.html

Putin, V. (2020). Statement by President of Russia Vladimir Putin on a Comprehensive Program of Measures for Restoring the Russia-US Cooperation in the Field of International Information Security. *The Kremlin.* Retrieved from http://en.kremlin.ru/events/president/news/64086

Putnam, R. D., Leonardi, R., & Nanetti, R. Y. (1994). *Making Democracy Work: Civic Traditions in Modern Italy*: Princeton University Press.

Qiu, J. L. (2003). The Internet in China: Data and Issues. *Annenberg Research Seminar on International Communication.* Retrieved from http://www.arnic.info/Papers/JQ_China_and_Internet.pdf

QuoIntelligence. (2020). APT28 Delivers Zebrocy Malware Campaign using NATO Theme as Lure. *QuoIntelligence.* Retrieved from https://quointelligence.eu/2020/09/apt28-zebrocy-malware-campaign-nato-theme/

Radin, A., & Reach, C. (2017). Russian Views of the International Order. *RAND Corporation.* Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1800/RR1826/RAND_RR1826.pdf

Rafsky, S. (2011). At Occupy Protests, U.S. Journalists Arrested, Assaulted. *Committee to Protect Journalists.* Retrieved from https://cpj.org/2011/11/at-occupy-protests-us-journalists-arrested-assault/

Raiu, C., & Kuznetsov, I. (2015). Comparing the Regin Module 50251 and the "Qwerty" Keylogger. *SecureList by Kaspersky.* Retrieved from https://securelist.com/comparing-the-regin-module-50251-and-the-qwerty-keylogger/68525/

Rattray, G. J. (2001). *Strategic Warfare in Cyberspace*. Cambridge: MIT Press.

Rauch, J. (2018). The Constitution of Knowledge. *National Affairs.* Retrieved from https://www.nationalaffairs.com/publications/detail/the-constitution-of-knowledge

Redick, J. R., Carasales, J. C., & Wrobel, P. S. (1995). Nuclear Rapprochement: Argentina, Brazil, and the Nonproliferation Regime. *Washington Quarterly, 18*(1), 107-122.

Reed, J. (2015). Unit 8200: Israel's Cyber Spy Agency. *Financial Times.* Retrieved from https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c

Reid, M. (2014). *Brazil: The Troubled Rise of a Global Power*. New Haven: Yale University Press.

Rekow, L. (2016). Pacification & Mega-Events in Rio de Janeiro: Urbanization, Public Security & Accumulation by Dispossession. *Journal of Human Security, 12*(1).

Reuters. (2008a). Russia Army Vows Steps if Georgia and Ukraine Join NATO. *Reuters.* Retrieved from https://www.reuters.com/article/us-russia-nato-steps-idUSL1143027920080411

Reuters. (2008b). U.S. Military Stretched Dangerously Thin by War: Poll. *Reuters.* Retrieved from https://www.reuters.com/article/us-usa-military-survey/u-s-military-stretched-dangerously-thin-by-war-poll-idUSN1930361920080219

Reuters. (2014). State Department's Unclassified Email Systems Hacked. *Reuters.* Retrieved from https://www.reuters.com/article/us-cybersecurity-statedept-idUSKCN0J11BR20141117

Reuters. (2015). Russia Suspected in Cyber Attack on U.S. Military Email. *Reuters.* Retrieved from https://www.reuters.com/article/usa-military-cyberattack-idINKCN0QB2CH20150806

Reuters. (2017). LinkedIn Fails to Agree with Russia on Restoring Access to Site. *Reuters.* Retrieved from https://www.reuters.com/article/us-linkedin-russia-ban-idUSKBN16E20Q

Reuters. (2018). Latvia Says Russia Targeted its Foreign and Defense Bodies with Cyber Attacks. *Reuters.* Retrieved from https://www.reuters.com/article/us-latvia-russia-cyber-idUSKCN1MI1SB

Reuters. (2020). Russia Lifts Ban on Telegram Messaging App After Failing to Block It. *Reuters.* Retrieved from https://www.reuters.com/article/us-russia-telegram-ban-idUSKBN23P2FT

Rhodin, S. (2008). Hackers Tag Lithuanian Web Sites With Soviet Symbols. *The New York Times.* Retrieved from https://www.nytimes.com/2008/07/01/world/europe/01baltic.html

Ricupero, R. (2010). Brasil: Potência de Paz ou de Guerra? *Folha de S.Paulo.* Retrieved from https://www1.folha.uol.com.br/fsp/dinheiro/fi1104201006.htm

Rid, T. (2011). Cyber War Will Not Take Place. *Journal of Strategic Studies, 35*(1), 5-32.

Rid, T. (2013). *Cyber War Will Not Take Place*. Oxford: Oxford University Press.

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux.

Rid, T. (2022). Why You Haven't Heard About the Secret Cyberwar in Ukraine. *The New York Times.* Retrieved from https://www.nytimes.com/2022/03/18/opinion/cyberwar-ukraine-russia.html

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies, 38*(1-2), 4-37.

Riley, M. (2014). NSA Said to Have Used Heartbleed Bug, Exposing Consumers. *Bloomberg News.* Retrieved from https://www.bloomberg.com/news/articles/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers

Ripsman, N. M., Taliaferro, J. W., & Lobell, S. E. (2016). *Neoclassical Realist Theory of International Politics*. New York: Oxford University Press.

Roache, M. (2019). Breaking Down the Complicated Relationship Between Russia and NATO. *Time.* Retrieved from https://time.com/5564207/russia-nato-relationship/

Roberts, H., Zuckerman, E., York, J., Faris, R., & Palfrey, J. (2010). Circumvention Tool Usage Report. *Berkman Center for Internet & Society.* Retrieved from https://cyber.harvard.edu/sites/cyber.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf

Rogers, M. (2014). Why the Sony Hack Is Unlikely to Be the Work of North Korea. *Marc's Security Ramblings.* Retrieved from http://marcrogers.org/2014/12/18/why-the-sony-hack-is-unlikely-to-be-the-work-of-north-korea/

Roguski, P. (2020). Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace. *Just Security.* Retrieved from https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/

Rohr, A. (2012). Anonymous Ataca Sites Ligados ao Governo em Protesto Contra a Rio+20. *G1.* Retrieved from http://g1.globo.com/tecnologia/noticia/2012/06/anonymous-ataca-sites-ligados-ao-governo-em-protesto-contra-rio20.html

Romanosky, S., & Boudreaux, B. (2019). Private Sector Attribution of Cyber Incidents. *RAND Corporation.*

Root. (2019). ETERNALBLUE, Conducting a History Lesson in Exploitation. *Root.* Retrieved from https://rootsecdev.medium.com/eternalblue-conducting-a-history-lesson-in-exploitation-fd06a7cf41d5

Rose, G. (1998). Neoclassical Realism and Theories of Foreign Policy. *World Politics, 51*(1), 144-172.

Rosecrance, R. N. (1987). *The Rise of the Trading State: Commerce and Conquest in the Modern World*. New York: Basic Books.

Rosecrance, R. N. (1996). The Rise of the Virtual State. *Foreign Affairs, 75*(4), 45-61.

Rosecrance, R. N. (1999). *The Rise of the Virtual State: Wealth and Power in the Coming Century*. New York: Basic Books.

Rosecrance, R. N. (2002). International Security and the Virtual State: States and Firms in World Politics. *Review of International Studies, 28*(3), 443-455.

Rosen, N. (2005). If America Left Iraq. *The Atlantic.* Retrieved from https://www.theatlantic.com/magazine/archive/2005/12/if-america-left-iraq/304412/

Rosenau, J. N. (1969). *Linkage Politics: Essays on the Convergence of National and International Systems*. New York: The Free Press.

Rosenbach, E., & Peritz, A. J. (2009). Confrontation or Collaboration? Congress and the Intelligence Community. *Belfer Center for Science and International Affairs.* Retrieved from https://www.belfercenter.org/sites/default/files/files/publication/cuber-security.pdf

Rosenberg, E. (2018). Twitter to Tell 677,000 Users They Were Had by the Russians. Some Signs Show the Problem Continues. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/to-hunt-osama-bin-laden-satellites-watched-over-abbottabad-pakistan-and-navy-seals/2013/08/29/8d32c1d6-10d5-11e3-b4cb-fd7ce041d814_story.html

Ross, A. (2010). Internet Freedom: Historic Roots and the Road Forward. *SAIS Review of International Affairs, 30*(2), 3-15.

Ross, W. (2020). Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States. *US Department of Commerce.* Retrieved from https://www.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect

Rossi, A. (2018). How the Snowden Revelations Saved the EU General Data Protection Regulation. *The International Spectator, 53*(4), 95-111.

Rousseff, D. (2013). Speech by President Dilma Rousseff on the occasion of the General Debate of the 68th General Assembly of the United Nations – New York, 24 September 24, 2013. *Executive Branch of the Government of Brazil.* Retrieved from https://www.gov.br/mre/en/content-centers/speeches-articles-and-interviews/president-of-the-federative-republic-of-brazil/speeches/statement-by-the-president-of-the-federative-republic-of-brazil-dilma-rousseff-at-the-general-debate-of-the-69th-general-assembly-of-the-united-nations-new-york-september-24th-2014

Ruggie, J. G. (1998). What Makes the World Hang Together? Neo-Utilitarianism and the Social Constructivist Challenge. *International Organization, 52*(4), 855-885.

Russell, A. L. (2014). *Cyber Blockades*. Washington DC: Georgetown University Press.

Rustici, R. M. (2011). Cyberweapons: Leveling the International Playing Field. *Parameters, 41*(3), 12.

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet, 11*(4), 89.

Salehan, M., & Negahban, A. (2013). Social Networking on Smartphones: When Mobile Phones Become Addictive. *Computers in Human Behavior, 29*(6), 2632-2639.

Salinas, S. (2018). Six top US intelligence chiefs caution against buying Huawei phones. *CNBC.* Retrieved from https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html

Sanchez, R. (2014). Tweeting at Terrorists: Inside America's Social Media Battle With Online Jihad. *The Telegraph.* Retrieved from https://www.telegraph.co.uk/news/worldnews/al-qaeda/10829355/Tweeting-at-terrorists-inside-Americas-social-media-battle-with-online-jihad.html

Sanger, D. E. (2009). U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site. *The New York Times.* Retrieved from https://www.nytimes.com/2009/01/11/washington/11iran.html

Sanger, D. E. (2012a). *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Random House.

Sanger, D. E. (2012b). Mutually Assured Cyberdestruction? *The New York Times.* Retrieved from https://www.nytimes.com/2012/06/03/sunday-review/mutually-assured-cyberdestruction.html

Sanger, D. E. (2012c). Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times.* Retrieved from http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Sanger, D. E. (2016a). Obama Strikes Back at Russia for Election Hacking. *The New York Times.* Retrieved from https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html

Sanger, D. E. (2016b). U.S. Cyberattacks Target ISIS in a New Line of Combat. *The New York Times.* Retrieved from https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html

Sanger, D. E. (2016c). U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam. *The New York Times.* Retrieved from https://www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyberattacks-on-banks-and-a-dam.html

Sanger, D. E. (2018). *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York: Crown.

Sanger, D. E., & Broad, W. J. (2017). Trump Inherits a Secret Cyberwar Against North Korean Missiles. *The New York Times.* Retrieved from https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html

Sanger, D. E., & Fackler, M. (2015). N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say. *The New York Times.* Retrieved from https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html

Sanger, D. E., & Mazzetti, M. (2016). U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict. *The New York Times.* Retrieved from https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html

Sanger, D. E., & Perlroth, N. (2014). U.S. Denies It Knew of Heartbleed Bug on the Web. *The New York Times.* Retrieved from https://www.nytimes.com/2014/04/12/us/us-denies-knowledge-of-heartbleed-bug-on-the-web.html

Sanger, D. E., & Perlroth, N. (2019). U.S. Escalates Online Attacks on Russia's Power Grid. *The New York Times.* Retrieved from https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

Sanger, D. E., Perlroth, N., & Schmitt, M. N. (2021). Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit. *The New York Times.* Retrieved from https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html

Sanger, D. E., & Rappeport, A. (2021). Treasury Department's Senior Leaders Were Targeted by Hacking. *The New York Times.* Retrieved from https://www.nytimes.com/2020/12/21/us/politics/russia-hack-treasury.html

Sanger, D. E., & Schmitt, E. (2017). U.S. Cyberweapons, Used Against Iran and North Korea, Are a Disappointment Against ISIS. *The New York Times.* Retrieved from https://www.nytimes.com/2017/06/12/world/middleeast/isis-cyber.html

Sanovich, S. (2018). Russia: The Origins of Digital Misinformation. In S. C. Woolley & P. N. Howard (Eds.), *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (pp. 21-40). Oxford: Oxford University Press.

Sappington, D. E. M. (1991). Incentives in Principal-Agent Relationships. *Journal of Economic Perspectives, 5*(2), 45-66.

Savage, C. (2018). Justice Dept. Revives Push to Mandate a Way to Unlock Phones. *The New York Times.* Retrieved from https://www.nytimes.com/2018/03/24/us/politics/unlock-phones-encryption.html

Savchuk, L. (2017). My Life as a Troll - Lyudmila Savchuk's Story. *Danish Institute for International Studies.* Retrieved from https://www.diis.dk/en/my-life-as-a-troll-lyudmila-savchuk-s-story

Scahill, J., & Greenwald, G. (2014). The NSA's Secret Role in the U.S. Assassination Program. *The Intercept.* Retrieved from https://theintercept.com/2014/02/10/the-nsas-secret-role/

Schelling, T. C. (1966). *Arms and Influence*. New Haven: Yale University Press.

Schmidt, A. (2013). The Estonian Cyberattacks. In J. Healey (Ed.), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (pp. 174-193). Washington DC: Cyber Conflict Studies Association.

Schmidt , M. S., & Sanger, D. E. (2015). Russian Hackers Read Obama's Unclassified Emails, Officials Say. *The New York Times.* Retrieved from https://www.nytimes.com/2015/04/26/us/russian-hackers-read-obamas-unclassified-emails-officials-say.html

Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.

Schneider, J. (2020). A Strategic Cyber No-First-Use Policy? Addressing the US Cyber Strategy Problem. *The Washington Quarterly, 43*(2), 159-175.

Schneier, B. (2012). *Liars and Outliers: Enabling the Trust that Society Needs to Thrive*. Cambridge: Polity Press.

Schneier, B. (2014). Heartbleed. *Schneier on Security.* Retrieved from https://www.schneier.com/blog/archives/2014/04/heartbleed.html

Schneier, B. (2015). Did North Korea Really Attack Sony? *The Atlantic.* Retrieved from https://www.theatlantic.com/international/archive/2014/12/did-north-korea-really-attack-sony/383973/

Schneier, B. (2016a). The NSA Is Hoarding Vulnerabilities. *Schneier on Security.* Retrieved from https://www.schneier.com/blog/archives/2016/08/the_nsa_is_hoar.html

Schneier, B. (2016b). The Value of Encryption. *Schneier on Security.* Retrieved from https://www.schneier.com/essays/archives/2016/04/the_value_of_encrypt.html

Schoka, A. (2019). Cyber Command, the NSA, and Operating in Cyberspace: Time to End the Dual Hat. *War on the Rocks.* Retrieved from https://warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/

Schwartz, A., & Knake, R. K. (2016). Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process. *Belfer Center for Science and International Affairs.* Retrieved from https://www.belfercenter.org/sites/default/files/files/publication/Vulnerability%20Disclosure%20Web-Final4.pdf

Schweller, R. L. (2004). Unanswered Threats: A Neoclassical Realist Theory of Underbalancing. *International Security, 29*(2), 159-201.

Schweller, R. L. (2009). Neoclassical Realism and State Mobilization: Expansionist Ideology in the Age of Mass Politics. In S. Lobell, N. Ripsman, & J. W. Taliaferro (Eds.), *Neoclassical Realism, the State, and Foreign Policy*. New York: Cambridge University Press.

Schweller, R. L. (2011). Emerging Powers in an Age of Disorder. *Global Governance, 17*, 285.

Seddon, M. (2014). Documents Show How Russia's Troll Army Hit America. *BuzzFeed News.* Retrieved from https://www.buzzfeednews.com/article/maxseddon/documents-show-how-russias-troll-army-hit-america

Sedler, R. A. (2006). An Essay on Freedom of Speech: The United States versus the Rest of the World Essay. *Michigan State Law Review, 2006*(2), 377-384.

Segal, A. (2016). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York: PublicAffairs.

Segal, A. (2017). Tracking State-Sponsored Cyber Operations. *Council on Foreign Relations.* Retrieved from https://www.cfr.org/blog/tracking-state-sponsored-cyber-operations

Sesek, R. (2014). Unraveling NSA's TURBULENCE Programs. *Robert Sesek.* Retrieved from https://robert.sesek.com/2014/9/unraveling_nsa_s_turbulence_programs.html

Shachtman, N. (2010). Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack (Updated). *Wired.* Retrieved from https://www.wired.com/2010/08/insiders-doubt-2008-pentagon-hack-was-foreign-spy-attack/

Shaffer, K. (2017). Spot a Bot: Identifying Automation and Disinformation on Social Media. *Medium.* Retrieved from https://medium.com/data-for-democracy/spot-a-bot-identifying-automation-and-disinformation-on-social-media-2966ad93a203

Shane, S., & Perlroth, N. (2019). N.S.A. Denies Its Cyberweapon Was Used in Baltimore Attack, Congressman Says. *The New York Times.* Retrieved from https://www.nytimes.com/2019/05/31/us/nsa-baltimore-ransomware.html

Shane, S., Perlroth, N., & Sanger, D. E. (2017). Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core. *The New York Times.* Retrieved from https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html

Shane, S., & Sreenivasan, H. (2019). American Towns Under Cyberattack From an NSA-Built Software. *PBS.* Retrieved from https://www.pbs.org/newshour/show/american-towns-under-cyberattack-from-an-nsa-built-software

Sheldon, J. B. (2014). Geopolitics and Cyber Power: Why Geography Still Matters. *American Foreign Policy Interests, 36*(5), 286-293.

Sherlock, T. (2019). Russian Society and Foreign Policy: Mass and Elite Orientations After Crimea. *Problems of Post-Communism, 67*(1), 1-23.

Sherman, W. R. (2018). How We Got the Iran Deal: And Why We'll Miss It Essays. *Foreign Affairs, 97*(5), 186-198.

Shifrinson, J. R. I. (2016). Deal or No Deal? The End of the Cold War and the US Offer to Limit NATO Expansion. *International Security, 40*(4), 7-44.

Shires, J., & Smeets, M. (2017). The Word Cyber Now Means Everything - and Nothing At All. *Slate.* Retrieved from http://www.slate.com/blogs/future_tense/2017/12/01/the_word_cyber_has_lost_all_meaning.html

SIDtoday. (2009). What Are the Latest SIGINT Developments in Iraq and Afghanistan? An Interview with Colonel Parker Schenecker. *SIDtoday.* Retrieved from https://theswissbay.ch/pdf/NSA/The%20Intercept/sidtoday/documents/2009/2009-10-21_SIDToday_-_What_Are_the_Latest_SIGINT_Developments_in_Iraq_and_Afghanistan_An_Interview_with_Colonel_Parker_Schenecker.pdf

Sigholm, J. (2016). Non-State Actors in Cyberspace Operations. *Journal of Military Studies, 4*(1), 1-37.

Silove, N. (2018). Beyond the Buzzword: The Three Meanings of "Grand Strategy". *Security Studies, 27*(1), 27-57.

Silver, N. (2018a). For Instance, This Story Makes a Big Deal About a (Post-election) Russian Social Media Disinformation Campaign on Bob Mueller Based on… 5,000 Tweets? *Twitter.* Retrieved from https://twitter.com/NateSilver538/status/1074833714931224582

Silver, N. (2018b). How Much Did Russian Interference Affect The 2016 Election? *FiveThirtyEight.* Retrieved from https://fivethirtyeight.com/features/how-much-did-russian-interference-affect-the-2016-election/

Silver, N. (2018c). If You Wrote Out a List of the Most Important Factors in the 2016 Election, I'm Not Sure That Russian Social Media Memes Would Be Among the Top 100. *Twitter.* Retrieved from https://twitter.com/NateSilver538/status/1074833714931224582

Simmons, B. A. (1999). *Territorial Disputes and Their Resolution: The Case of Ecuador and Peru* (Vol. 27). Washington DC: United States Institute of Peace.

Sindjoun, L. (2001). Transformation of International Relations: Between Change and Continuity: Introduction. *International Political Science Review / Revue Internationale de Science Politique, 22*(3), 219-228.

Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The Weaponization of Social Media*. Boston: Eamon Dolan.

Singer, P. W., & Cole, A. (2015). *Ghost Fleet: A Novel of the Next World War*. Boston: Eamon Dolan.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What Everyone Needs to Know*. New York: Oxford University Press.

SIPRI. (2022). SIPRI Military Expenditure Database. *Stockholm International Peace Research Institute.* Retrieved from https://milex.sipri.org/sipri

Skinner, B. F. (1965). *Science And Human Behavior*. New York: The Free Press.

Smeets, M. (2018). A Matter of Time: On the Transitory Nature of Cyberweapons. *Journal of Strategic Studies, 41*(1-2), 6-32.

Smith, B. (2017). The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack. *Microsoft On the Issues.* Retrieved from https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/

Snowden, E. (2019). *Permanent Record*. New York: Picador.

Snyder, G. H. (1965). The Balance of Terror and the Balance of Power. In P. Seabury (Ed.), *The Balance of Power* (pp. 184–201). San Francisco: Chandler.

Sobelman, D. (2018). Restraining an Ally: Israel, the United States, and Iran's Nuclear Program, 2011-2012. *Texas National Security Review, 1*(4), 11-38.

Solar, C. (2020). Cybersecurity and Cyber Defence in the Emerging Democracies. *Journal of Cyber Policy, 5*(3), 392-412.

Sood, K., & Hurley, S. (2017). NotPetya Technical Analysis - A Triple Threat: File Encryption, MFT Encryption, Credential Theft. *CrowdStrike Blog.* Retrieved from https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/

Soshnikov, A. (2017). Inside a Pro-Russia Propaganda Machine in Ukraine. *BBC News.* Retrieved from https://www.bbc.com/news/blogs-trending-41915295

Sottek, T. C. (2012). Google Executive Arrested in Brazil as the Company Resists Orders to Freeze Political Speech on YouTube. *The Verge.* Retrieved from https://www.theverge.com/2012/9/26/3413476/google-brazil-you-tube-arrest

Sreeharsha, V. (2016). WhatsApp Blocked in Brazil as Judge Seeks Data. *The New York Times.* Retrieved from https://www.nytimes.com/2016/05/03/technology/judge-seeking-data-shuts-down-whatsapp-in-brazil.html

Srivastava, A., Morris, T., Ernster, T., Vellaithurai, C., Pan, S., & Adhikari, U. (2013). Modeling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information. *IEEE Transactions on Smart Grid, 4*(1), 235-244.

St. Augustine. (1952). *Treatises on Various Subjects (The Fathers of the Church, Volume 16)*: Catholic University of America Press.

Stanley, D. (2003). What Do We Know about Social Cohesion: The Research Perspective of the Federal Government's Social Cohesion Research Network. *The Canadian Journal of Sociology / Cahiers Canadiens de Sociologie, 28*(1), 5-17.

START. (2019). Global Terrorism Database. *National Consortium for the Study of Terrorism and Responses to Terrorism.* Retrieved from https://www.start.umd.edu/gtd

State.gov. (2006a). Global Internet Freedom Task Force. *US Department of State.* Retrieved from https://2001-2009.state.gov/g/drl/lbr/c26696.htm

State.gov. (2006b). Global Internet Freedom Task Force (GIFT) Strategy: A Blueprint for Action. *US Department of State.* Retrieved from https://2001-2009.state.gov/g/drl/rls/78340.htm

Steil, B. (2013). *The Battle of Bretton Woods: John Maynard Keynes, Harry Dexter White, and the Making of a New World Order*. Princeton: Princeton University Press.

Stephen, M. D. (2012). Rising Regional Powers and International Institutions: The Foreign Policy Orientations of India, Brazil and South Africa. *Global Society, 26*(3), 289-309.

Stern, J. (2015). Obama and Terrorism: Like It or Not, the War Goes On. *Foreign Affairs, 94*(5), 62-70.

Stewart, L. G., Arif, A., & Starbird, K. (2018). *Examining Trolls and Polarization with a Retweet Network.* Paper presented at the Misinformation and Misbehavior Mining on the Web (MIS2).

Stratfor. (2012). *Emerging Economies: The Geopolitics of the BRICS Nations*. Austin: Stratfor.

Stronski, P., & Sokolsky, R. (2020). Multipolarity in Practice: Understanding Russia's Engagement With Regional Institutions. *Carnegie Endowment for International Peace.* Retrieved from https://carnegieendowment.org/files/Stronski_Sokolsky_Multipolarity_final.pdf

Suebsaeng, A. (2014). The State Department Is Actively Trolling Terrorists on Twitter. *Mother Jones.* Retrieved from https://www.motherjones.com/politics/2014/03/state-department-cscc-troll-terrorists-twitter-think-again-turn-away/

Sullivan, A. (2009). The Revolution Will Be Twittered. *The Atlantic.* Retrieved from https://www.theatlantic.com/daily-dish/archive/2009/06/the-revolution-will-be-twittered/200478/

Swisher, C. (2015). The Spy Cables: A Glimpse Into the World of Espionage. *Al Jazeera.* Retrieved from https://www.aljazeera.com/news/2015/02/spy-cables-world-espionage-snowden-guardian-mi6-cia-ssa-mossad-iran-southafrica-leak-150218100147229.html

Symantec. (2011). W32.Stuxnet Dossier. *Symantec.* Retrieved from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Symantec. (2019). Internet Security Threat Report. *Symantec.* Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

T., J. E. (2017). The Tallinn Manual 2.0: Highlights and Insights. *Georgetown Journal of International Law, 48*, 735-778.

Tabansky, L. (2016). *Towards a Theory of Cyber Power: The Israeli Experience with Innovation and Strategy.* Paper presented at the 8th International Conference on Cyber Conflict (CyCon).

Tabansky, L., & Israel, I. B. (2015). *Cybersecurity in Israel*. Cham: Springer.

Taleb, N. N. (2008). *The Black Swan: The Impact of the Highly Improbable*. London: Penguin Books.

Taleb, N. N. (2013). Hormesis Is Redundancy. In J. Brockman (Ed.), *This Explains Everything: 150 Deep, Beautiful, and Elegant Theories of How the World Works*. New York: Harper Perennial.

Taliaferro, J. W. (2006). State Building for Future Wars: Neoclassical Realism and the Resource-Extractive State. *Security Studies, 15*(3), 464-495.

Taliaferro, J. W., Lobell, S., & Ripsman, N. (2009). Introduction: Neoclassical Realism, the State, and Foreign Policy. In S. Lobell, N. Ripsman, & J. Taliaferro (Eds.), *Neoclassical Realism, the State, and Foreign Policy*. New York: Cambridge University Press.

Taylor, A. M. (1992). External Dependence, Demographic Burdens, and Argentine Economic Decline After the Belle Époque. *The Journal of Economic History, 52*(4), 907-936.

Temperton, J. (2020). How the 5G Coronavirus Conspiracy Theory Tore Through the Internet. *Wired UK.* Retrieved from https://www.wired.co.uk/article/5g-coronavirus-conspiracy-theory

Temple-Raston, D. (2019). How The U.S. Hacked ISIS. *NPR.* Retrieved from https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis

Thomas, T. L. (2000). The Russian View of Information War. In M. H. Crutcher (Ed.), *The Russian Armed Forces at the Dawn of the Millennium* (pp. 335-360). Carlisle: US Army War College.

Thompson, N. B., & Muggah, R. (2016). With Anonymous' Latest Attacks in Rio, the Digital Games Have Begun. *openDemocracy.* Retrieved from https://www.opendemocracy.net/en/with-anonymous-latest-attacks-in-rio-digital-games-have-begun/

Thompson, P. (2007). The Case of the Missing Hegemon: British Nonintervention in the American Civil War. *Security Studies, 16*(1), 96-132.

Thompson, S. K., Landgren, K., & Romita, P. (2022). The United Nations in Hindsight: Challenging the Power of the Security Council Veto. *Just Security.* Retrieved from https://www.justsecurity.org/81294/the-united-nations-in-hindsight-challenging-the-power-of-the-security-council-veto/

ThreatConnect. (2016). Shiny Object? Guccifer 2.0 and the DNC Breach. *ThreatConnect.* Retrieved from https://threatconnect.com/blog/guccifer-2-0-dnc-breach/

Thrush, G., & Davenport, C. (2017). Donald Trump Budget Slashes Funds for E.P.A. and State Department. *The New York Times.* Retrieved from https://www.nytimes.com/2017/03/15/us/politics/budget-epa-state-department-cuts.html

Thucydides. (2009). *The Peloponnesian War*. Oxford: Oxford University Press.

Timberg, C., & Miller, G. (2014). FBI Blasts Apple, Google for Locking Police Out of Phones. *The Washington Post.* Retrieved from https://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html

Traynor, I. (2007). Russia Accused of Unleashing Cyberwar to Disable Estonia. *The Guardian.* Retrieved from https://www.theguardian.com/world/2007/may/17/topstories3.russia

Trenin, D. (2009). Russia in the Caucasus: Reversing the Tide. *The Brown Journal of World Affairs, 15*(2), 143-155.

Trenin, D. V. (2011). *Post-Imperium: A Eurasian Story*. Washington DC: Carnegie Endowment for International Peace.

Trinkunas, H. (2015). Brazil's Global Ambitions. *Brookings Institution.* Retrieved from https://www.brookings.edu/articles/brazils-global-ambitions/

Trinkunas, H., & Wallace, I. (2015). Converging on the Future of Global Internet Governance: The United States and Brazil. *Brookings Institution.* Retrieved from https://www.brookings.edu/wp-content/uploads/2016/06/usbrazil-global-internet-governance-web-final.pdf

Trubowitz, P. (1998). *Defining the National Interest: Conflict and Change in American Foreign Policy*. Chicago: University of Chicago Press.

Trump, D. J. (2019). Remarks by President Trump to the 74th Session of the United Nations General Assembly. *The White House.* Retrieved from https://trumpwhitehouse.archives.gov/briefings-statements/remarks-president-trump-74th-session-united-nations-general-assembly/

Tuchman, B. W. (1985). *The Zimmermann Telegram*. New York: Random House.

Tufekci, Z. (2018). It's The (Democracy-Poisoning) Golden Age Of Free Speech. *Wired.* Retrieved from https://www.wired.com/story/free-speech-issue-tech-turmoil-new-censorship/

Twenge, J. M., Joiner, T. E., Rogers, M. L., & Martin, G. N. (2017). Increases in Depressive Symptoms, Suicide-Related Outcomes, and Suicide Rates Among U.S. Adolescents After 2010 and Links to Increased New Media Screen Time. *Clinical Psychological Science, 6*(1), 3-17.

Uchill, J. (2017). No Evidence of Russia Behind Macron Leaks: Report. *The Hill.* Retrieved from https://thehill.com/policy/cybersecurity/336034-no-evidence-of-russia-behind-marcon-leaks-report/

United States of America. (2017). Vulnerabilities Equities Policy and Process for the United States Government. *The White House.* Retrieved from https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

United States of America. (2018). National Cyber Strategy of the United States of America. *The White House.* Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

United States Senate. (2019). Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election: Volume 2: Russia's Use of Social Media, with Additional Views. *Select Committee on Intelligence*

United States Senate. Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

United States Senate. (2020). Diplomacy in Crisis: The Trump Administration's Decimation of the State Department. *Democratic Staff on the Senate Foreign Relations Committee.* Retrieved from https://www.foreign.senate.gov/download/2020-sfrc-minority-report_-diplomacy-in-crisis----the-trump-administrations-decimation-of-the-state-department

Vaidhyanathan, S. (2018). *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy*. New York: Oxford University Press.

Vaishnav, C., Choucri, N., & Clark, D. (2013). Cyber International Relations as an Integrated System. *Environment Systems and Decisions, 33*(4), 561-576.

Valeriano, B. G., Jensen, B. M., & Maness, R. C. (2018). *Cyber Strategy: The Evolving Character of Power and Coercion*. New York: Oxford University Press.

Valeriano, B. G., Lonergan, E. D., W., L. S., & Jensen, B. M. (2022). Putin's Invasion of Ukraine Didn't Rely on Cyberwarfare. Here's Why. *Cato Institute.* Retrieved from https://www.cato.org/commentary/putins-invasion-ukraine-didnt-rely-cyberwarfare-heres-why

Valeriano, B. G., & Maness, R. C. (2014). The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011. *Journal of Peace Research, 51*(3), 347-360.

Valeriano, B. G., & Maness, R. C. (2015). *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. Oxford: Oxford University Press.

Valeriano, B. G., & Maness, R. C. (2016). Cyber Spillover Conflicts: Transitions from Cyber Conflict to Conventional Foreign Policy Disputes? In K. Friis & J. Ringsmose (Eds.), *Conflict in Cyber Space* (pp. 61-80): Routledge.

van der Spuy, A. (2017). *What If We All Governed the Internet? Advancing Multistakeholder Participation In Internet Governance*. Paris: UNESCO.

van Prooijen, J.-W., & Douglas, K. M. (2018). Belief on Conspiracy Theories: Basic Principles of an Emerging Research Domain. *European journal of social psychology, 48*(7), 897-908.

Vandewalker, I. (2013). Since Citizens United, a Decade of Super PACs. *Brennan Center for Justice.* Retrieved from https://www.brennancenter.org/our-work/analysis-opinion/citizens-united-decade-super-pacs

Vargina, V. (2020). Sputnik V Vaccine as a Soft-Power Instrument of Russia. *Journal of Governance and Politics, 2*(7), 2020-2027.

Vigevani, T., & Fernandes de Oliveira, M. (2007). Brazilian Foreign Policy in the Cardoso Era: The Search for Autonomy Through Integration. *Latin American Perspectives, 34*(5), 58-80.

Vilmer, J.-B. J. (2019). The "#Macron leaks" Operation: A Post-Mortem. *Atlantic Council.* Retrieved from https://www.atlanticcouncil.org/in-depth-research-reports/report/the-macron-leaks-operation-a-post-mortem/

Vine, D. (2015). *Base Nation: How U.S. Military Bases Abroad Harm America and the World*. New York: Henry Holt & Company.

VirusBlokAda. (2010). Rootkit.TmpHider. *VirusBlokAda.* Retrieved from http://anti-virus.by/en/tempo.shtml

Voltmer, K. (2010). The Media, Government Accountability, and Citizen Engagement. In P. Norris (Ed.), *Public Sentinel: News Media and Governance Reform*. Washington DC: World Bank Publications.

von Clausewitz, C. (2008). *On War*. Princeton: Princeton University Press.

Vosoughi, S., Roy, D., & Aral, S. (2018). The Spread of True and False News Online. *Science, 359*(6380), 1146-1151.

Wahal, A. (2022). On International Treaties, the United States Refuses to Play Ball. *Council on Foreign Relations.* Retrieved from https://www.cfr.org/blog/international-treaties-united-states-refuses-play-ball

Waldman, A. E. (2017). The Marketplace of Fake News Symposium: Hate Crime v. Hate Speech: Exploring the First Amendment. *University of Pennsylvania Journal of Constitutional Law, 20*(4), 845-870.

Walker, P. (2014). North Korea Internet Service Resumes After Shutdown. *The Guardian.* Retrieved from https://www.theguardian.com/world/2014/dec/23/north-korea-internet-shutdown

Walt, S. M. (2012). What if Realists Were in Charge of U.S. Foreign Policy? *Foreign Policy.* Retrieved from https://foreignpolicy.com/2012/04/30/what-if-realists-were-in-charge-of-u-s-foreign-policy/

Walt, S. M. (2018). *The Hell of Good Intentions: America's Foreign Policy Elite and the Decline of U.S. Primacy*. New York: Farrar, Straus and Giroux.

Waltz, K. N. (1959). *Man, the State, and War: A Theoretical Analysis*. New York: Columbia University Press.

Waltz, K. N. (1979). *Theory of International Politics*. Boston: McGraw-Hill.

Waltz, K. N. (2000). NATO Expansion: A Realist's View. *Contemporary Security Policy, 21*(2), 23-38.

Washington, G. (1796). Farewell Address. *The American Presidency Project.* Retrieved from https://www.presidency.ucsb.edu/documents/farewell-address

Waterman, S. (2007). Analysis: Who Cyber Smacked Estonia? *UPI.* Retrieved from https://www.upi.com/Defense-News/2007/06/11/Analysis-Who-cyber-smacked-Estonia/26831181580439/

Watterson, C. J. (2017). Competing Interpretations of the Stability-Instability Paradox: The Case of the Kargil War. *The Nonproliferation Review, 24*(1-2), 83-99.

Watts, J. (2015). Judge Lifts Whatsapp Ban In Brazil After Ruling Block Punished Users Unfairly. *The Guardian.* Retrieved from https://www.theguardian.com/world/2015/dec/17/brazil-whatsapp-ban-lifted-facebook

Way, L. A., & Casey, A. E. (2019). *How Can We Know if Russia is a Threat to Western Democracy? Understanding the Impact of Russia's Second Wave of Election Interference.* Paper presented at the Conference on Global Populisms and their International Diffusion.

We Are Social. (2022). Digital 2022: Brazil. *We Are Social.* Retrieved from https://datareportal.com/reports/digital-2022-brazil

Webb, A. (2017). Cold War Radio and the Hungarian Uprising, 1956. In L. Risso (Ed.), *Radio Wars: Broadcasting During the Cold War*. Abingdon: Routledge.

Weber, V. (2018). Linking Cyber Strategy with Grand Strategy: The Case of the United States. *Journal of Cyber Policy, 3*(2), 236-257.

Weiffen, B., Wehner, L., & Nolte, D. (2013). Overlapping Regional Security Institutions in South America: The Case of OAS and UNASUR. *International Area Studies Review, 16*(4), 370-389.

Weimann, G. (2005). Cyberterrorism: The Sum of All Fears? *Studies in Conflict & Terrorism, 28*(2), 129-149.

Weisman, S. R. (2005). U.S. Expands Aid to Iran's Democracy Advocates Abroad. *The New York Times.* Retrieved from https://www.nytimes.com/2005/05/29/world/middleeast/us-expands-aid-to-irans-democracy-advocates-abroad.html

Wendt, A. (1992). Anarchy is what States Make of it: The Social Construction of Power Politics. *International Organization, 46*(2), 391-425.

Wendt, A. (1995). Constructing International Politics. *International Security, 20*(1), 71-81.

Wendt, A. (1999). *Social Theory of International Politics*. Cambridge: Cambridge University Press.

Wendt, A. (2004). The State as Person in International Theory. *Review of International Studies, 30*(2), 289-316.

Weyland, K. (2016). Realism Under Hegemony: Theorizing the Rise of Brazil. *Journal of Politics in Latin America, 8*(2), 143-173.

Wheeler, D. A., & Larsen, G. N. (2003). *Techniques for Cyber Attack Attribution*. Alexandria: Institute for Defense Analyses.

Whigham, T. L., & Potthast, B. (1999). The Paraguayan Rosetta Stone: New Insights Into the Demographics of the Paraguayan War, 1864-1870. *Latin American Research Review, 34*(1), 174-186.

Whillans, A. V., & Chen, F. S. (2018). Facebook Undermines the Social Belonging of First Year Students. *Personality and Individual Differences, 133*, 13-16.

White, S. P. (2018). Understanding Cyberwarfare: Lessons from the Russia-Georgia War. *Modern War Institute.* Retrieved from https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/

Whitehead, T. (2015). Internet Firms to Be Banned From Offering Unbreakable Encryption Under New Laws. *The Telegraph.* Retrieved from https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11970391/Internet-firms-to-be-banned-from-offering-out-of-reach-communications-under-new-laws.html

Whitlock, C., & Gellman, B. (2013). To Hunt Osama bin Laden, Satellites Watched Over Abbottabad, Pakistan, and Navy SEALs. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/to-hunt-osama-bin-laden-satellites-watched-over-abbottabad-pakistan-and-navy-seals/2013/08/29/8d32c1d6-10d5-11e3-b4cb-fd7ce041d814_story.html

WikiLeaks. (2016). DNC Email Archive. *WikiLeaks.* Retrieved from https://wikileaks.org/dnc-emails/

WikiLeaks. (2017). Vault 7: CIA Hacking Tools Revealed. *WikiLeaks.* Retrieved from https://wikileaks.org/ciav7p1/#PRESS

Wilcox, H., Bhattacharya, M., & Islam, R. (2014). *Social Engineering Through Social Media: An Investigation on Enterprise Security.* Paper presented at the International Conference on Applications and Techniques in Information Security (ATIS).

Wilson, S. (2020). SolarWinds Recap: All of the Federal Agencies Caught up in the Orion Breach. *FedScoop.* Retrieved from https://www.fedscoop.com/solarwinds-recap-federal-agencies-caught-orion-breach/

Wohlforth, W. C. (2008). Realism. In C. Reus-Smit & D. Snidal (Eds.), *The Oxford Handbook of International Relations* (pp. 131-149). Oxford: Oxford University Press.

Wohlstetter, A. (1958). The Delicate Balance of Terror. *Foreign Affairs, 37*(2), 211-234.

Wong, D., & Chadwick, S. (2017). Risk and (In)security of FIFA Football World Cups - Outlook for Russia 2018. *Sport in Society, 20*(5-6), 583-598.

Wonnell, C. T. (1985). Truth and the Marketplace of Ideas. *U.C. Davis Law Review, 19*(3), 669-728.

Woo, S., & Morris, B. (2018). AT&T Backs Off Deal to Sell Smartphones From China's Huawei. *The Wall Street Journal.* Retrieved from https://www.wsj.com/articles/at-t-backs-off-deal-to-sell-smartphones-from-chinas-huawei-1515443153

World Bank. (2016). How the Internet Promotes Development. *World Bank.* Retrieved from http://documents.worldbank.org/curated/en/896971468194972881/310436360_20160263021502/additional/102725-PUB-Replacement-PUBLIC.pdf

World Bank. (2020). World Bank Country and Lending Groups. *World Bank.* Retrieved from https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups

Wutz, I., & Nugteren, L. (2018). Brexit and Online Political Activism: On Vox Populism, Slacktivism and Online Intertextuality. *Diggit Magazine.* Retrieved from https://www.diggitmagazine.com/papers/brexit-and-online-political-activism

Yablokov, I. (2021). How The Kremlin's Years of Conspiracy Spreading Are Biting Back. *Moscow Times.* Retrieved from https://www.themoscowtimes.com/2021/03/01/how-the-kremlins-years-of-conspiracy-spreading-are-biting-back-a73111

Yardley, H. O. (1931). *The American Black Chamber*. Indianapolis: Bobbs-Merrill Company.

Yuan, L. (2018). A Generation Grows Up in China Without Google, Facebook or Twitter. *The New York Times.* Retrieved from https://www.nytimes.com/2018/08/06/technology/china-generation-blocked-internet.html

Zaharna, R. S. (2004). From Propaganda to Public Diplomacy in the Information Age. In Y. R. Kamalipour & N. Snow (Eds.), *War, Media, and Propaganda: A Global Perspective*. Lanham: Rowman & Littlefield.

Zajko, M. (2018). Security against Surveillance: IT Security as Resistance to Pervasive Surveillance. *Surveillance & Society, 16*(1), 39-52.

Zakaria, F. (2011). *The Post-American World* (2nd ed.). New York: W. W. Norton & Company.

Zeldin, W. (2012). U.N. Human Rights Council: First Resolution on Internet Free Speech. *Library of Congress.* Retrieved from https://www.loc.gov/law/foreign-news/article/u-n-human-rights-council-first-resolution-on-internet-free-speech/

Zetter, K. (2011). How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. *Ars Technica.* Retrieved from https://arstechnica.com/tech-policy/2011/07/how-digital-detectives-deciphered-stuxnet-the-most-menacing-malware-in-history/

Zetter, K. (2014a). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers.

Zetter, K. (2014b). How to Detect Sneaky NSA 'Quantum Insert' Attacks. *Wired.* Retrieved from https://www.wired.com/2015/04/researchers-uncover-method-detect-nsa-quantum-insert-hacks/

Zetter, K. (2014c). U.S. Gov Insists It Doesn't Stockpile Zero-Day Exploits to Hack Enemies. *Wired.* Retrieved from https://www.wired.com/2014/11/michael-daniel-no-zero-day-stockpile/

Zetter, K. (2016). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *Wired.* Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Ziegler, C. E. (2021). A Crisis of Diverging Perspectives: US-Russian Relations and the Security Dilemma. *Texas National Security Review, 4*(1), 12-33.

Zinets, N. (2016). Ukraine Hit by 6,500 Hack Attacks, Sees Russian 'Cyberwar'. *Reuters.* Retrieved from https://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC

Zubok, V. M. (2009). *A Failed Empire: The Soviet Union in the Cold War from Stalin to Gorbachev*. Chapel Hill: University of North Carolina Press.