June 2020

A Dangerous New Era: Analyzing the Impact of Cyber Technology on International Conflict

Kenneth Brown
University of South Florida

A Dangerous New Era:

Analyzing the Impact of Cyber Technology on International Conflict

by

Kenneth Brown

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy in Politics and International Affairs
with a concentration in International Relations
Department of Government and International Affairs
College of Arts and Sciences
University of South Florida

Major Professor: Jongseok Woo, Ph.D.
Bernd Reiter, Ph.D.
Nicolas Thompson, Ph.D.
Keenan Yoho, Ph.D.

Date of Approval:
June 15, 2020

Keywords: cyberattack, espionage, propaganda, United States, Russia, Vladimir Putin

Table of Contents

List of Tables

List of Diagrams

Abstract

This paper examines the causal relationship between cyber technology's deep global integration and changes in how states struggle for power in the international system. Specifically, it argues that cyber technology has changed international conflict by providing external actors the ability to penetrate states' grand strategy decision-making and implementation processes to an unprecedented degree and scope. As a result, the meaning of power has changed from a material-centric metric to one that is more nuanced and difficult to measure.

To explore this hypothesis, the study follows a three-step process. First, it examines the history of cyber technology, how it has become deeply embedded within the modern state, and the vulnerabilities this has created. Second, to set the foundation for a comparative analysis, the paper uses a neoclassical realist framework to conduct case studies of US and Soviet / Russian grand strategies in the Cold War (1980s) and New Era of Conflict (2007-2018), highlighting the role of cyber technology in the latter. Third, the study compares the cases to gain an understanding of the differences in international conflict between the eras. The paper then synthesizes these results with evidence of the state's exploitation of cyber-related vulnerabilities, to draw conclusions on how cyber technology has impacted international conflict.

Collectively, these steps not only validate the hypothesis, but they also raise fundamental questions about current international relations theory and highlight important implications for US national security policy. In addition, by examining cyber technology's impacts holistically, applying neoclassical realist theory in a novel way, and using a broad definition for international conflict, the paper expands theory application and fills a significant gap in the current literature.

Chapter One: Introduction

Problem Statement

Over the past thirty years, cyber technology has infiltrated nearly every aspect of our daily lives. Often, its presence is unknown or taken for granted, as we unwittingly rely on it to operate our vehicles, talk with family members, control the household temperature, or cook meals. This is no less true at the state level, where basic functions, such as utilities, elections, finances, and communications all depend on networked computer systems, sensors, and data to ensure their efficient and effective functioning.

Although cyber technology's ubiquity has generated many benefits, its deep integration and importance to modern society have also created extensive vulnerabilities that malign actors have recognized and actively attempted to exploit. As a result, over the past two decades the world has witnessed a myriad of operations by intelligence organizations, military units, and sponsored contractors which have taken advantage of inherent weaknesses to steal sensitive information, damage important data, attack others' infrastructures, and manipulate their populations. Much like other inventions throughout history, therefore, cyber technology has become yet another capability for states to use in their enduring struggle for power.

At the same time, international conflict has undergone dramatic changes, as China, Russia, and the United States have engaged in an increasingly contentious battle to determine who will lead the international system and the shape it will take. In the process, these and other states have used their capabilities in sometimes unique ways that have challenged our understanding of the character of conflict and the nature of power itself. As a result, scholars have struggled to understand how conflict is evolving, as the distinction between peace and war has blurred, long-standing norms have been undermined, and traditional metrics of power have been brought into question.

While it is evident that dramatic changes have occurred in international conflict, it is unclear how much of a role cyber technology has played in the process. This is not to say that there is a lack of evidence that states have been exploiting the technology to achieve their goals. Examples such as the US-attributed Stuxnet cyberattack that destroyed an estimated 1,000 Iranian centrifuges, Russian hack and release operations against the 2016 US and French elections, and China's notoriously aggressive cyber espionage campaign all point to cyber-based vulnerabilities and successful attempts to exploit them. However, states have been engaging in sabotage, espionage, and propaganda operations for eons, which means that a cause and effect relationship between cyber technology and changes in international conflict cannot be presupposed. This puzzle will be the focus of my study.

Despite scholars' extensive research into the impact of cyber technology on international conflict, the topic nonetheless largely remains controversial and unsettled. From some scholars' perspectives, for instance, the real and potential effects are overstated, while others argue that cyber technology has greatly affected how states struggle for power. Unfortunately, the scholars' conclusions are often based on poorly defined terms and they focus heavily on the destructive potential of cyberattacks. As a result, existing studies tend to underestimate the potential effects of other nefarious activities, such as when actors use the technology to exacerbate social divisions or obtain and release sensitive information. In addition, even when scholars examine these risks, they typically do so in a segmented rather than holistic fashion. Thus, the literature generally lacks a comprehensive analysis of how cyber technology is being used by states in their struggle for power and the changes these actions have caused to international conflict.

Summary of Main Argument

To address the literature gap, this project will conduct a comparative case study analysis of international conflicts in pre and post cyber eras to identify changes that have occurred and discover cyber technology's role in the process. Specifically, to understand conflict's evolution, I will examine how the US and Russia used their elements of power to achieve their grand strategic goals during the 1980s and the 2007-2018 timeframe. In addition, I will conduct a detailed analysis of the vulnerabilities that the cyber revolution has created. By ultimately comparing these findings with the evidence on how the US and Russia have modified their approaches over time, and highlighting the ways they have exploited the identified cyber-related vulnerabilities to achieve their objectives, I will identify how cyber technology has changed international conflict, at least as it relates to these two states.

Collectively these steps provide the requisite framework for examining my hypothesis that cyber technology has had a fundamental impact on international conflict and the meaning of power in the Twenty-First Century. Specifically, I argue that, by providing states with the ability to create direct and indirect effects on their adversaries' decision-making and implementation processes, to a unique scope and degree, cyber technology has fundamentally changed the ways states struggle for power. Moreover, due to cyber capabilities' minimal attributability, intangible nature, and substantial effects, the meaning of power has changed from a material-centric concept to one that is more nuanced and difficult to measure. As a result, cyber technology has impacted states' means of engaging in conflict and greatly complicated the calculation of relative power in the international system.

Significance and Contribution

As will be explained in the final chapter, the project not only validates my arguments, but my findings demonstrate that the effects of the revolution in cyber technology expand well beyond them. Specifically, as a key component within states' governments, physical infrastructures, societies, and economies, cyber technology has become a great enabler for all their elements of power. Therefore, those states best able to protect their vulnerabilities while using their cyber capabilities to exploit their adversaries' will gain a substantial advantage in international conflict. Moreover, in my analysis of the states' grand strategies, I find that the United States has been far less successful than Russia in adjusting its grand strategy and integrating the full scope of cyber capabilities.

These findings raise fundamental questions about international relations theory, states' national security investments, and defense strategies. As a result, the study provides a substantial contribution not only by helping to close the literature gap discussed above, but also by highlighting some of the inherent risks of not making the adjustments to the US grand strategy necessary to address the changes in power that have occurred over the past twenty years.

Summary of Chapters

This study contains five substantive chapters. In the first, I provide a detailed explanation of my theory and research design. As part of this I explain my methodology, outline my theoretical framework, and define key terms. Through this process, I describe my theory in detail and explain how I use neoclassical realism to identify vulnerabilities resident within states' decision-making processes. In addition, I conduct a short literature review in which I discuss existing thoughts on my research question and identify gaps. Taken together, these steps set the analytical and theoretical frameworks for my subsequent data collection and analysis.

In the second chapter, I provide a detailed overview of cyber technology's history, explore the changes it has created, and examine the resulting vulnerabilities. To support this step, I use process tracing to show how key events set the foundations for the internet's rapid growth from a government run, internal collaboration tool to a global network with an estimated four billion users (Bennett & Checkel 2015; Murphy & Roser 2017).

As part of this analysis, I trace developments forward in time to explore how the integration of cyber technology into everyday life and human behavior combined to create rapid growth, but also extensive vulnerabilities. For quantitative data, I use publicly available government and private industry resources, as well as existing literature. These include the National Institute of Standards and Technology (NIST) database on internet integration and vulnerabilities, as well as commercial sites that track the rates of global internet technology platforms' proliferation, regional and state penetration rates, and user demographics.

To complete this chapter, I explore how state and non-state actors have exploited cyber vulnerabilities to influence and undermine states' neoclassical realist intervening variables outlined above. For data, I use public documents, official statements, conference notes, and other scholars' analyses. While I draw on data from across the globe, to stay consistent with the case study approach, I focus primarily on Russia and the US.

In the third and fourth chapters I analyze the grand strategies the US and Russia adopted during the Cold War and the New Era of Conflict (2007-2018), respectively. To control for in case variation during the Cold War, I focus on the period 1980-1989. The timespan, which covers the Reagan administration, provides a relevant case due to the high level of tensions and attending maneuvers by the US and Soviet Union to enhance or preserve their power. This approach allows me to scope the field of study while also exploring two highly relevant periods of international conflict in which essentially the same states were involved.

Data sources include current and archival materials from online repositories, as well as government reports and scholarly studies. Throughout, I use neoclassical realist theory to assess the ways, means, and ends actors employed to achieve their goals by destroying, coercing, deterring, or manipulating target states' decision-making and implementation mechanisms. Although states often do not clearly articulate their grand strategies, they do follow a consistent set of policies that reflect an unstated framework (Trubowitz 2011: 9-10). As such, at times it is necessary to extrapolate the grand strategies from scholarly studies, official statements, documents, and state behaviors. In the process, I assess how those grand strategies evolved with time and examine their resulting impact on international conflict. In addition, in the second case study, I highlight how each state used cyber technology to exploit its opponent's decision-making vulnerabilities. As a final step in these chapters, I develop conceptual models for each period that visually depict the ways in which the states collectively employed their elements of power.

In the fifth chapter I compare the data generated by the above steps to discover how the grand strategies adopted by the US and Russia differed between the conflict periods. It is important to note, however, that since the topics of study present complex problems involving multiple interrelated variables, I do attempt to demonstrate specific causes as to why the states changed their grand strategies over time. Instead, to identify the role cyber technology played in this process, I synthesize the data on cyber vulnerabilities from Chapter Two with the results from the above comparison. Through these steps, I bring together the cyber-related vulnerabilities and state behavior, which allow me to draw conclusions on how cyber technology has impacted international conflict. As a final part of this chapter, I then explore the results' implications, identify gaps in my analysis, and discuss areas for further research.

Collectively, these steps provide a theoretically framed, empirically based approach that avoids the equifinality problem resident within such complex, evolving subjects. While gaps remain due to data limitations and the use of only two case studies, the project nonetheless greatly progresses thought on cyber technology, international conflict, and power in the Twenty-First Century.

Chapter Two: Theory, Literature Review, and Research Design

Introduction

Although international conflict has been a topic of study for millennia, due to the uncertainty of human behavior, changing technology, and the fluid nature of the international environment, its causes, conduct, and solutions remain contentious and opaque. Similarly, cyber technology's relative novelty, rapid evolution, and widespread integration into everyday life present a complex puzzle, the significance and impact of which scholars continue to debate. Thus, despite extensive scholarly analysis, international conflict and cyber technology remain controversial enigmas.

As a project focused on analyzing the impact of cyber technology on international conflict, therefore, this dissertation faces significant challenges with equifinality, definitional ambiguity, and limited evidence. At the same time, however, a well-constructed research design can mitigate these and other hurdles by applying rigorous methodological, theoretical, and epistemological criteria. Procedurally, this mandates a design founded on strict research objectives, clear variables, relevant cases, a well-defined unit of analysis, and solid empirical evidence, embedded within a rigorous method and a clear, relevant, and falsifiable theory (George & Bennett 2004: 74-88; King, Keohane, & Verba 1994: 100-114).

This project will meet these requirements by conducting a comparative analysis of conflict between Russia and the United States during the 1980s and the 2007-2018 timeframe.

Using qualitative and demonstrative quantitative data, analyzed through the lens of a neoclassical realist variant, I will examine the states' grand strategies as a metric of international conflict. By evaluating the differences between the states' grand strategies during pre and post internet periods, and highlighting how they adjusted their approaches due to the new technology, I will gain an understanding of how international conflict has evolved and the role cyber technology played in these developments. Taken together, these steps will provide the requisite framework for evaluating my theory that the revolution in cyber technology is changing international conflict by enabling actors to directly impact states' grand strategy formation and execution processes in historically novel ways.

In this chapter I describe the above approach in detail. Specifically, I will first outline the study's theoretical model, explain why it was selected, discuss its variables and causal arguments, and describe how it will be employed throughout. With that framework established, I will then review the literature to demonstrate the current state of knowledge on the revolution in cyber technology and international conflict. In the process, I will also identify gaps, and explain how my research seeks to fill them. Third, I will describe the research design, which includes my theory, key definitions, data sources, and the methodology employed. Finally, I will outline my project's overall structure, with an overview of each chapter. Collectively, these steps will provide a detailed description of the approach taken, explain how it meets the above criteria, and will lay the foundation for the remainder of the paper.

Analytical Framework

As a project focused on understanding how international conflict has changed, this research will follow the realist paradigm in international relations. This school of thought operates on fundamental assumptions about the international system, in which the primary actors are unitary, rational states operating as like units in anarchy and responding to systemic forces defined in terms of relative material power (Waltz 1979).

Within the realist paradigm, however, there is a wide variation in interpretation of how these assumptions operate and where the emphasis should be placed. For instance, offensive and defensive realism argue that states respond to international stimuli by adopting aggressive, power maximization policies or pursuing strategies designed to protect their security, respectively (Mearsheimer 2001; Walt 1987). On the other hand, neoclassical realism, which is the theoretical framework used in this project, argues that, while systemic forces impact states' behavior, they do so through the "imperfect transmission belt" of domestic level intervening variables (Rose 1998; Schweller 2004). Therefore, rather than assuming that states respond automatically and optimally to changes in relative material power, neoclassical realism introduces unit level factors into the causal chain (He 2017: 137).

In addition to variations within the realist paradigm writ large, there are also multiple versions of neoclassical realism reflecting different degrees of complexity and explanatory power. Specifically, the original model posited by Rose and associated scholars includes two interrelated intervening variables: executive leaders' perceptions of relative power and their ability to access and employ the requisite resources necessary to carry out their foreign policy decisions (Rose 1998: 151-153; Zakaria 1998: 35-38). Kitchen, however, argues that strategic ideas alone provide the necessary explanatory factor (2010), while Ripsman, Taliaferro, and Lobell posit a theoretical framework based on four intervening variables, as well as structural modifiers and systemic variables (2016). These theories, however, are either incomplete or overly complex and therefore do not fully explain states' grand strategy selections in a sufficiently parsimonious manner.

To overcome this gap, this research uses a modified version of neoclassical realism that draws from several models. Specifically, the neoclassical realist variant used in this project posits that, while grand strategies are driven by systemic stimuli, the ultimate ways, means, and ends are shaped by three intervening variables: executive leaders' perceptions of the threat environment, their ability to access and employ the resources needed to implement their decisions, and the state's strategic culture. I will discuss each of these variables in turn.

Systemic Stimuli

According to realist theory, state behavior is driven primarily by relative material power capabilities within the anarchic international system (Rose 1998: 146). While neoclassical realists add unit level intervening variables to help explain states' ultimate behaviors, they largely follow the same core realist causal structure. This model, however, is incomplete in that it leaves open questions on how the term "international system" is defined and it adopts a narrow independent variable that does not account for how states detect and assess changes to material conditions (Ripsman, et. al. 2016: 34).

To address these gaps, Ripsman, Taliaferro, and Lobell argue for the addition of structural modifiers, such as technology diffusion rates, geography, and the offense-defense balance, as well as the systemic variables, clarity and environmental permissiveness (2016: 40-57). Although this version addresses the above gaps, it also adds substantial complexity to an already complicated model in which existing variables arguably account for such considerations. To mitigate these concerns, the theoretical framework used in this project defines the systemic stimuli broadly to encompass the elements of power, or means, available for a state's use in conflict. Thus, systemic stimuli are not limited solely to material power metrics, such as military and economic capabilities, but also include geography, technology, and ideological factors. Moreover, as for the other variables suggested by Ripsman, et. al, the model addresses them through the lens of the intervening variables, which carry much of the burden for influencing how states act.

Grand Strategy (Unit of Analysis)

Although the term "grand strategy" is used frequently by scholars, pundits, and policymakers, there is neither a single accepted definition nor agreement on the concept's utility (Balzacq, et. al. 2018: 1-2; Silove 2018: 27-28). To understand the dependent variable, therefore, it is important to clearly define the term and explain why grand strategy has been selected over other systemic outputs.

As used in this project, grand strategy is defined as the conceptual framework a foreign policy executive uses to align the ways and means of national security with its desired long-term goals and within the constraints of its available resources, ideas, and political will (Brands 2014, 3; Legro 2005). Thus, grand strategy is a holistic, enduring approach states employ in peace and war to most effectively and efficiently apply their national security assets to address perceived threats and exploit opportunities (Brooks & Wohlforth 2016,:75; Trubowitz 2011: 9-10).

Although some scholars argue that grand strategy is a questionable concept with limited utility, it nonetheless represents a useful metric for analyzing international conflict. Specifically, by evaluating how the ways, means, and ends states used to engage in the struggle for power changed over time, it is possible to trace the path of international conflict's evolution. The fact that the grand strategies often fail due to domestic resistance, resource limitations, or poor execution does not inure against this argument but rather reinforces the validity of the theoretical framework adopted herein. Moreover, while some neoclassical realist scholars identify foreign policy as the independent variable, such an approach is too limited in time and scope to meet this project's analytical needs. Rather, since grand strategy is the guiding framework for foreign policy and includes both internal and external considerations, it is a superior unit of analysis for measuring how states engage in international conflict.

Intervening Variables

Leaders' Perceptions of the Threat Environment

A nation's leadership is the focal point for national security decision-making. As such, the leaders' understanding of the security environment, particularly their perception of potential or existing threats, is likely to impart significant influence on the grand strategy each state adopts and how it is implemented. For the term leaders, this paper includes the designated head of the government as well as his or her principle advisors, cabinet members, and senior government officials who have influence over the information the head of government sees and hears, and who are primarily responsible for implementing decisions (Ripsman, et. al.: 61-62). How this foreign policy executive (FPE) sees the threat environment depends heavily upon its members' own experiences, education, and biases, the information they use, and the bureaucratic apparatuses that support them. As such, leaders' perceptions will evolve depending on who occupies the inner circle and how the underlying bureaucracy operates.

Leaders’ Ability to Access and Employ Resources

Government structure, economic conditions, and domestic political considerations all impact whether the leaders’ decisions can be implemented and in what forms. When the FPE enjoys centralized power, a unified government with extensive funding, and direct control over the implementation processes, its decisions will be executed more easily and accurately. On the other hand, a divided, resource poor government with a resistant bureaucracy and hostile political environment will face significant challenges in this regard (Rose 1998: 151-153; Zakaria 1998: 38-39). Since the government’s prosperity, domestic power, and structures evolve with time and circumstances, these factors are critical to understanding why a state adopts a certain grand strategy and how it implements it.

Strategic Culture

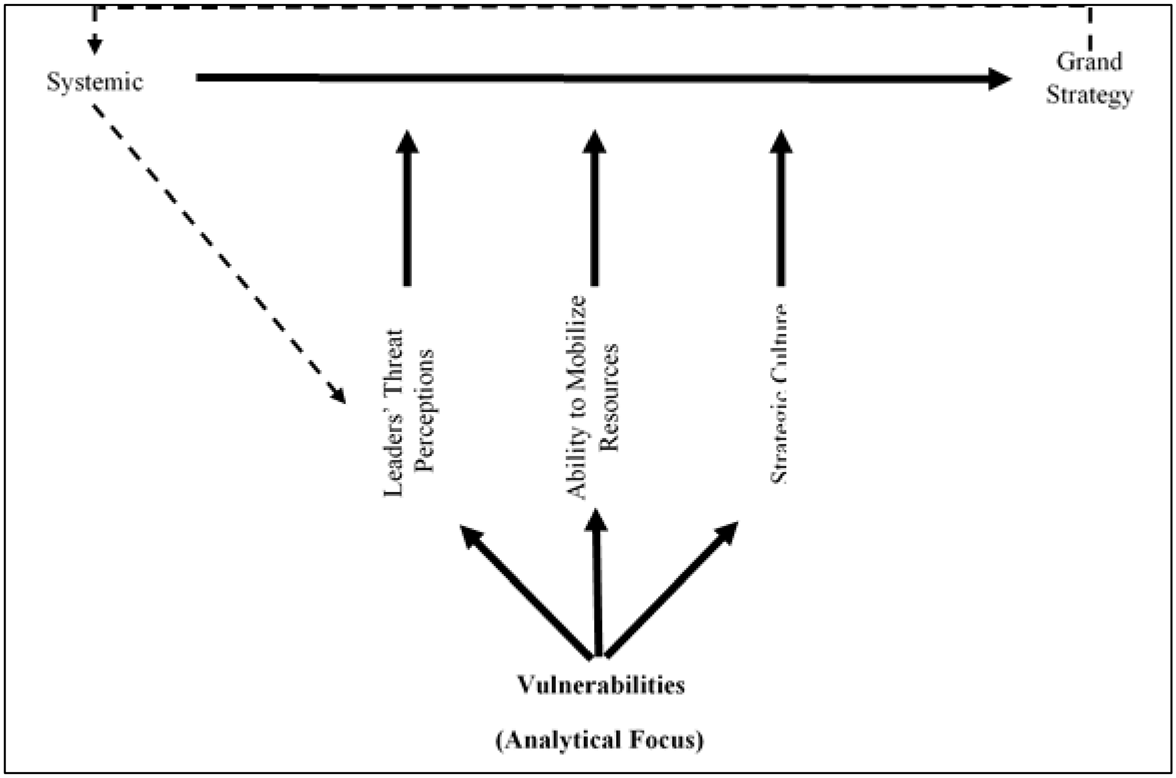
State behavior is also driven by its strategic culture, which is founded in its unique history, geography, shared values, and ideas (Kitchen 2010; Lantis 2014). These factors play a critical role in creating the lens through which leaders and other actors view and react to the world around them. As such, strategic culture is an important consideration when attempting to understand why states act differently than rational choice or structural models would predict. Although strategic culture is enduring, it can change slowly over time or rapidly due to shocks, such as foreign invasion, economic crisis, or civil war (Greathouse 2010). Therefore, to understand a state’s behavior, particularly its use of force, its extant strategic culture must be included in the analysis.

Through this process, the research ensures that international, state, and domestic considerations are taken into account while also maintaining a structured baseline. Although neoclassical realism does emphasize international systemic forces, this version also considers multiple internal factors that are embedded within the intervening variables outlined above. As such, this approach provides a superior framework compared with other forms of realism, as well as liberalism and constructivism variants, which generally privilege one of the three levels to the detriment of the others or adopt normative approaches while eschewing structural considerations.

In addition, the project's theoretical framework advances thought on neoclassical realism in two significant ways. First, by including strategic culture as an intervening variable, my approach accounts for sociocultural considerations and ideas, which are ignored in most realist constructs. In this way, the theory draws from Kitchen, which focuses on ideas as a critical component of state decision-making. At the same time, however, my approach strikes an apt balance between parsimony and explanatory power. In the process, it expands upon the frameworks posited by Zakaria, Rose, and Kitchen while adopting a much less complex structure than the paradigm proposed by Ripsman, Taliaferro, & Lobell.

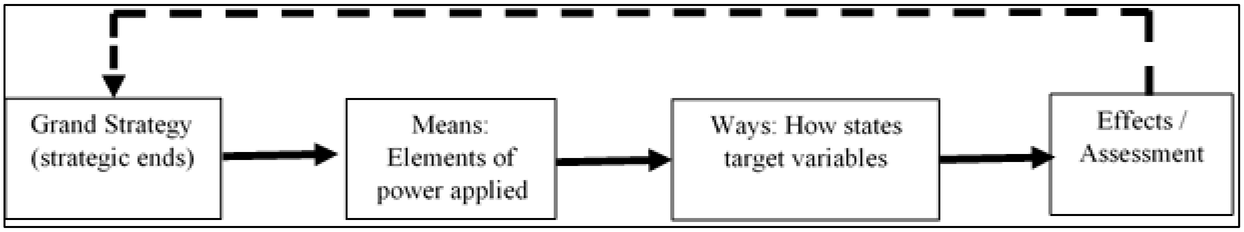
Second, and most importantly, I will employ the theory a unique way. Specifically, while neoclassical realism is commonly used to explain why states adopt certain foreign policies or grand strategies, in this project the theory will serve as the analytical lens for identifying the vulnerabilities in each state's decision-making processes and exploring its opponent's efforts to exploit them. As such, rather applying the theory to explain why the US and Russia adopted certain grand strategies, I will instead focus on how each state sought to use its elements of power to achieve its goals by manipulating its opponent's decision-making and implementation processes through the intervening variables.

Thus, in a marked difference from the existing literature, I will flip the theory on its head and use its central argument about state behaviors to expose US and Russian vulnerabilities and explore the methods each state used to attack them (Diagrams 1 and 2). Collectively, therefore, this project not only adds a balanced model to the existing literature, but it also expands neoclassical realism's potential explanatory power and creates a new avenue of analysis through which to explore how states engage in international conflict.



Neoclassical Realist Framework

Diagram 1


Grand Strategy (strategic ends)
Means: Elements of power applied
Ways: How states target variables
Effects / Assessment

Analytical Approach

Diagram 2

Literature Review

Since humans have been attempting to understand international conflict for thousands of years there is a massive amount of scholarly material on the subject. However, the volume can be narrowed considerably by assessing the literature through the lens of the study's purpose and theoretical framework. Thus, since my research is focused on evaluating how the revolution in cyber technology is changing international conflict, topics such as the causes of war or the preservation of peace can be eliminated at the outset. In addition, material focused exclusively on the tactical art of war, which falls below the strategic threshold, can be removed as well. Collectively, this culling process focuses the review on three remaining themes: 1) the evolution of conflict; 2) assessing actors' strategic approaches; and 3) the impact of cyber technology. Each of these is discussed in turn below.

The Evolution of Conflict

Within the literature on the conduct of war, there is a substantial debate over whether the nature of conflict evolves throughout history or is based upon unchanging principles that remain constant across the millennia (Milevski 2016). For instance, many scholars see Carl von Clausewitz' famous analysis of war as a fundamental precept that applies across space and time

(Smith 2005; Strachan & Scheipers 2011; Hoffman 2018). Others, however, argue that the principles are too vague to provide useful guidance to those making strategic decisions in the ever-changing circumstances of warfare (Brodie 1949; Alger 1982; Ali 2009). Adding complexity to the debate, scholars are often careful to distinguish between the character and the nature of war, with the former defined by the unique attributes of the participants, location, and technology, and the latter as an immutable condition reflected in war's inherent violence (Cebrowski 2005; Norwood, Jensen, & Barnes 2016). Moreover, Freedman argues that even defining war has become increasingly difficult due to changes in technology and actors use of approaches that defy traditional standards (Freedman 2017).

While these scholars raise important questions about the nature of warfare, their focus on war as a violent confrontation is much narrower than the scope of conflict as defined in this research. Specifically, they focus on the military elements of national power and thus downplay other critical tools. In addition, the scholars often conflate operational art with strategy, and therefore focus on specific campaigns or battles that fall below the grand strategic level of analysis. Although these details can provide evidence of strategic application, they are not strategies in and of themselves. Thus, while there is a vast amount of information in these sources to support the project's analysis, due to the broad definition of conflict I employ, no existing literature directly addresses the subject of my study.

In addition to the above, my research shares common ground with the international relations literature, particularly the realist school of thought, which assumes that interstate behavior is inherently conflictual (Waltz 1979; Mearsheimer 2001; Ripsman, et. al. 2016). Realist literature, however, is generally focused on explaining systemic or individual state behaviors. As such, although realists and scholars from across the international relations spectrum often seek to understand the causes of war or the ways to preserve peace, they typically do not engage in microanalyses of the nature of conflict itself. For instance, while Waltz (1954), Doyle (1983), and Katzenstein (1996) conduct extensive analyses of war and national security from the realist, liberal, and constructivist perspectives, respectively, they primarily focus on understanding how and why violent conflicts occur rather than how they are conducted by the actors involved. Recent scholarship takes a similar approach in its analysis of the current world order and the role power, identity, economics, international institutions, and technology are playing in shaping the international system and the potential for conflict (Drum 2018; Chua 2018; Deudney & Ikenberry 2018; Kotkin 2018; Varghese 2018).

Collectively, therefore, the two bodies of literature on the nature of international conflict do not directly address the research topic. At the same time, however, since my research will explore periods of war and key historical events that have been the subject of scholars' in-depth analysis, the literature will provide valuable insights and frameworks for understanding what occurred and why.

Actors' Strategic Approaches

As discussed above, the primary metric this research will use to understand the evolving nature of international conflict will be the grand strategies adopted by the states involved. By assessing the actors' grand strategies, my research will gain an understanding of the ways, means, and ends chosen by the states and why they adopted them. Through this process, I will gain an appreciation for the nature of the conflict under analysis and, through comparison, an understanding of how conflict itself has evolved.

As with any significant historical events, there is a massive amount of literature assessing the strategies employed by the United States and the Soviet Union during the Cold War as well as today. For instance, John Gaddis and Andrei Kokoshin analyze US and Soviet Cold War strategies, their roots in history, and ultimate successes and failures, respectively (Gaddis 2005a; Kokoshin 1999). Brands also conducts a critical assessment of each US president's grand strategy from Truman to G.W. Bush, in the process offering valuable insights into their strengths and weaknesses (Brands 2014). Regarding nuclear weapons, Herman Kahn's influential work *On Thermonuclear War* provides critical insights into the thought processes relating to strategic deterrence and the ways leaders can mitigate risks of escalation and misunderstanding (1960). Finally, Leffler and Westad provide a broad-sweeping analysis of the Cold War period in their multivolume *The Cambridge History of the Cold War* (2010).

For the New Era of Conflict, there is also an extensive amount of literature on Russian and US strategies, their ways of war, and how they are evolving. For example, recent scholarship on Russia evaluates how it employed different resources as weapons (Blank & 2016; Giles 2016), its foreign policies in different regions (Freiré 2009; Götz 2015), new military doctrine (Kasapoglu 2015; Klein 2015), and Putin's strategic approaches and goals in general (Lomagin 2007; Donaldson & Nogee 2009; Kotkin 2016; Lukyanov 2016). Of particular interest to recent scholars is the so-called Gerasimov doctrine of non-linear warfare, in which Russia purportedly used a blend of unconventional approaches to undermine its adversaries and gain objectives below the threshold of war (Kasapoglu 2015; Klein 2015; Trenin 2016). According to these and other scholars, this is the doctrine Russia applied in eastern Ukraine and Crimea and is currently employing against the US and its allies in Europe.

US strategic approaches post 2007 have also been a significant focus of study. Most recently, scholars have conducted detailed assessments of Trump’s grand strategy and whether it reflects a change from previous approaches (Posen 2018; Dombrowski & Reich 2017). Obama’s grand strategy was also subject to substantial critical analysis, raising questions on whether one existed, and assessing policies regarding the “pivot to Asia,” “leading from behind,” and counterterrorism (Clarke & Ricketts 2017; Lieber 2016; Brooks & Wolhforth 2016; Drezner 2011). Other scholars have taken a broader approach, assessing the central tenets of US grand strategy over time, often arguing that the post-Cold War approach has been and continues to be excessively interventionist, unsustainable, and counterproductive (Posen 2013; Smith 2017).

Collectively, the literature provides extensive analyses of US and Russian grand strategies during the conflict periods under study. These and other sources, therefore, will provide useful insights into the ways, means, and ends selected and employed by the actors involved. At the same time, however, none of the literature conducts a comparative analysis across the periods of this project’s study based upon the conceptual definition of international conflict employed in this research. As such, while there is a substantial amount of insightful literature on the Cold War and New Era of Conflict, this project is unique in its scope, approach, and purpose.

The Impact of Cyber Technology

As with the study of war and US and Russian grand strategies, there is a large body of scholarship on cyber technology and international security. The literature, however, is dominated by debates over the potential for cyberwar and related definitional discussions. At one end of the spectrum are scholars like Erik Gartzke and Adam Liff, who argue that the risks of cyber conflict are more hyperbolic that real (Gartzke 2013; Liff 2012). According to these scholars, concerns about catastrophic events, such as a cyber "Pearl Harbor," overstate the risks and erroneously conflate capability and intent (Gartzke 2013: 60-63).

Toward the center of the spectrum are scholars such as Lucas Kello and Thomas Rid, who recognize the risks of cyber conflict, but find that it is insufficiently violent or destructive to be considered "war" (Kello 2017: 52; Rid 2013: 3-10). For example, Kello, who provides one of the most comprehensive analyses of cyber technology's impact on the international order, concludes that it poses a real and significant threat to security, but that cyberwar is nonetheless highly unlikely (52). Jarno Limnéll likewise posits that cyber technology is a useful in warfare, although it is not as destructive as other capabilities (2015). This is similar to the position held by other scholars, including James Farwell and Rafal Rohozinski (2011), P.W. Singer and Allan Friedman (2014), and John Stone (2013), who argue that cyberwar is an unlikely occurrence due to the inability of associated capabilities to inflict death and destruction at any significant scale.

At the other end of the spectrum from Gartze and Liff, are scholars such as Nathalie Caplan (2013), Richard Clarke and Robert Knake (2010), Gary McGraw (2013), and John Arquilla and David Ronfelt (1997), who argue that cyberwar poses significant destructive and disruptive threats. According to this school of thought, not only is cyberwar real, but it is already happening and likely will increase in severity with time (Clarke & Knake 2010: 30-32).

It is important to note, however, that this apparent disparity in view is not as wide at it first appears. Rather, much of the difference is driven by incongruent uses of the term "cyberwar" (Eun & Abmann 2016: 346-348). As a result, even where scholars use the same underlying data, their conclusions on the threats posed by cyber technology differ due to how they implicitly define key words. Unfortunately, this remains a problem, as an attempt by Michael Robinson, Kevin Jones, and Helge Janicke to address the definitional inconsistency only complicated matters (2015).

Even when scholars use the same definitions, however, they tend to focus on cyberattacks and their potential rather than taking a holistic perspective of the technology within the larger schema of international conflict. For example, despite Kello's extensive analysis of the cyber revolution, he largely fails to account for the potential disruptive effects posed by social media and the ideological penetration of a state's society (Kello 2017). Similarly, while Johan Eriksson argues that power in the digital age is contextual rather than material, he likewise focuses on cyberattacks and vulnerabilities (Eriksson 2007). Although the potential nefarious influences of cyber-based psychological manipulation, espionage, and other nondestructive actions are examined by other scholars, the literature generally lacks a comprehensive analysis of cyber technology's impact on national security (Alarid 2009; Fidler 2012; Lindsay & Cheung 2015; Rudner 2017; Patrikarakos 2017; Singer & Brooking 2018).

Two exceptions to this segmented approach are Nazli Choucri and Joseph Nye, who take a holistic approach to assessing cyber technology's impact on the international system. Their analyses, however, are focused on how cyber technology influences power distribution and international relations theory, respectively. As such, they do not delve deeply into how cyber technology is impacting international conflict (Choucri 2012; Nye 2011). In addition, while Segal and Sanger engage in broad sweeping discussions of the ways state and non-state actors are using cyber technology, they do not synthesize the information into a comprehensive assessment of how these developments collectively implicate state security (Segal 2017; Sanger

2018). Therefore, the literature falls short in conducting a thorough and holistic assessment of how cyber technology is impacting international conflict.

Moreover, theory application is lacking since few scholars have analyzed the revolution in cyber technology through a theoretical lens. Within this select group, most focus on the offense-defense balance, with the majority agreeing that cyberspace is offense dominant due to its rapidly evolving nature, complexity, ease of access, and limited attributability (Kello 2017, 68; Saltzman 2013; Nye 2011). In addition, Kello argues that the intangible and unverifiable nature of cyber weapons exacerbates the security dilemma and the attending risk for conflict, while Saltzman argues that offense-defense theory is an outdated concept in the cyber era (Kello 2013: 32-33; Saltzman 2013).

Jon Lindsay, however, offers a different perspective in his assertion that cyberspace is defensively dominant. Specifically, Lindsay argues that cyber technology's offensive capabilities are overstated, which creates an increased risk of conflict due to state miscalculation (Lindsay 2015: 29). Libicki likewise argues that cyberspace is defensively dominant but based on the idea that it is a relatively weak domain relative to other weapons and that is incapable of denying actors access to actors' conventional or nuclear systems (Libicki 2011: 73).

From a different perspective, Chourci examines how cyber technology is impacting international relations theory writ large. Based on his analysis of current theoretical frameworks, he finds that they do not provide sufficient explanatory power. As an alternative, Chourci argues that lateral pressure theory offers the best approach to understanding how states behave in cyberspace (Choucri 2012). While Choucri discusses cyber technology, theory, and international conflict, his analysis is at the macro level and largely focused on defining terms (2012: 125-153). Thus, he only touches the surface of the interplay between technology and conflict.

Based upon the above review, it is evident that, while the literature provides a significant amount of data to support this research, it also suffers from substantive shortfalls. Specifically, due to scholars' focus on warfare, military science, and kinetic effects, much of the literature does not holistically address the phenomenon under consideration. In addition, the literature is often limited by the scope of analysis and the definitions employed.

This project will address these gaps in several ways. First, I will take a holistic approach that examines cyber technology's collective impact on international conflict. Thus, rather than focusing on a particular effect, I will conduct a broad-sweeping examination of the multiple ways cyber technology is changing conflict. Second, to ensure that readers understand the criteria behind my analysis, I will clearly define the terms I employ. Third, these definitions will be purposely broad, so as to encompass the multiple manifestations of cyber technology rather than viewing them through a limited and confusing lens. Finally, while I will not examine cyber technology's impact on international relations theory writ large, I will use a specific theoretical framework to provide analytical structure. In the process, I will add to an area of literature in which relatively little research has been conducted. Collectively, these steps will directly address many of the gaps identified above and thus will contribute to the literature by adding a much-needed holistic analysis, within a structured theoretical framework, based on clearly defined and broadly delimited terms.

To ensure that I achieve these goals and the project's broader objectives, I will focus on four research questions in the course of the study. Specifically: 1) How has great power conflict evolved over the past forty years?; 2) What factors influenced these changes?; 3) What role did cyber technology play in this process?; and 4) What conclusions can we draw on the implications of these changes for current policies and future developments? Together, these questions inform my research design, which is outlined in the next section.

Theory

My theory is that the revolution in cyber technology (independent variable) is changing international conflict (dependent variable) by enabling actors to directly impact states' grand strategy formation and execution processes in historically novel ways. Specifically, I argue that, due to cyber technology's deep integration into modern society, it has generated extensive vulnerabilities across the modern state's physical, societal, economic, and government structures. These vulnerabilities, in turn, provide external actors the unprecedented ability to directly penetrate states and undermine their power through novel, rapidly evolving, globally capable, and minimally attributable methods.

Moreover, I argue that cyber technology's intangible nature and potential impacts have undermined traditional metrics of power, thereby shifting its meaning from a material-centered concept to one that is more nuanced and difficult to measure. This development raises fundamental challenges for state decision-makers, who are charged with understanding and aptly adjusting their strategies to address perceived risks and opportunities across all operating domains. Thus, where the meaning and uses of power are obscure, it is difficult to the Foreign Policy Executive to achieve these goals.

Within this theory several terms require definition. First, as used in the project cyber is any technology connected to the internet, directly or indirectly (Clarke & Knake 2007: 69). Thus, the term includes any device with internet capability, such as automobiles, appliances, and industrial control mechanisms, as well as networks that have been “air gapped” or separated from direct connection through encrypted firewalls (Kello 2017: 45). Similarly, the revolution in cyber technology is defined as any changes that have occurred in the development and use of these capabilities, particularly in the past decade.

Second, international conflict is defined broadly as the adversarial struggle among actors to achieve their objectives within the international system. The term is not limited to “armed conflict,” but also involves all methods, such as espionage, propaganda, data manipulation, and sabotage. Finally, power includes the material and intangible factors that impact a state’s ability to achieve its objectives. Thus, in this study, the term is used in the context of a state’s elements of national power, which are means to an end and involve more than just material capabilities (Ripsman, et. al. 2016: 44).

Collectively, the theory and attending definitions directly address the literature gap identified above and challenge many of the underlying assumptions scholars have made regarding international conflict and cyber technology. In the process, rather than adopting the widely accepted material view of power that inherently drives a violence-based definition of conflict, my research employs a broader perspective. This approach allows for a more thorough and up to date examination of international conflict which is based on a struggle for power that extends well beyond the traditional model in which military and economic capabilities are given primacy.

Research Design: Cases, Methods, and Data

To explore my hypothesis, I conduct qualitative historical comparative analysis of international conflict across two cases: the Cold War and the ongoing new era of conflict that started in 2007. Since these cases represent incidents of international conflict between the same actors in pre and post internet eras, they provide the conditions for a natural experiment on the role cyber technology has played in state struggles for power.

To support these studies, I use qualitative and demonstrative quantitative data from official government and corporate reports, scholarly studies, primary materials, and online databases such as wearesocial.com and statistica.com. Methodologically, I use process tracing to show how events connected over time to create subsequent conditions (Bennett & Checkel 2015). Taken together, these data and methods provide a solid foundation for empirical examination of the historical evolution of international conflict over the past forty years, how it has changed, and the role cyber technology has played in the process.

Conclusion

This chapter provided an overview of the methodology, definitions, theory, research questions, and data sources used throughout the project. In addition, it reviewed the extant literature and outlined the paper's ultimate structure and contents. Through this process, the chapter explained how each element of the research design fits together to provide a holistic framework to support the resulting empirical analysis of how the revolution in cyber technology is changing international conflict.

Although a substantial amount of literature has been written about conflict and cyber technology, scholars have generally taken a narrow, violence-centric perspective or have addressed the topics in a segmented and therefore incomplete fashion. As a result, there is a substantial gap in understanding as to how international conflict is evolving and the role cyber technology is playing in states' struggles for power.

Through this research I seek to address these gaps by conducting a comparative case study of the grand strategies the US and Russia adopted during the Reagan Administration (1980-1989) and the New Era of Conflict, which I argue started in 2007 with Russia's cyberattacks on Estonia. Focusing on these actors' grand strategies during these periods, not only allows me to take advantage of a natural experiment involving essentially the same states in the pre and post cyber eras, but also enables a comparison of the ways, means, and ends each state adopted. In the process, I employ unique approaches such as espousing a broad, non-material centric definition of international conflict and conducting a holistic analysis of cyber technology in which physical, psychological, social, and other impacts are all taken into account.

For a theoretical lens, I use a neoclassical realism variant built around a causal chain in which international systemic stimuli drive states' grand strategies through three intervening variables: leaders' threat perspectives, their ability to mobilize resources, and the state's strategic culture. While this theory provides a framework for exploring the driving forces behind each state's grand strategic decisions, in this study it serves primarily as an assessment mechanism for the state's vulnerabilities, which are represented by the intervening variables. Thus, rather than attempting to deconstruct the grand strategies to identify specific causal mechanisms, which would be an impossible task due to the interrelated multivariate nature of the problem, I employ the theory as a lens through which to examine the strategies' intended impacts. Collectively this approach and the novel definitions expand the research beyond the existing literature and provide a solid framework for understanding how cyber technology has impacted the states' struggles for power.

To conduct the analysis, I follow three steps. First, to understand the variable, the project explores how the revolution in cyber technology has evolved and become integrated into everyday life and state apparatuses. In addition, I identify the vulnerabilities this integration has created and how state and non-state actors are exploiting them to undermine target states and societies. For data, I use qualitative and demonstrative quantitative evidence drawn from primary and secondary academic, corporate, and government sources. I then analyze these data through process tracing to show how events tied together over time to create the resulting conditions.

Second, using primary and secondary historical sources, I analyze the grand strategies adopted by the US and Russia during the Reagan Administration and the first decade of the New Era of Conflict. Each of these case studies demonstrates how the states employed their capabilities and resources in the struggle for power and thus provide critical evidence of how international conflict has evolved over the past forty years. As part of this process, I also specifically highlight how the states employed cyber technology as part of their grand strategies in the New Ear of Conflict. Based on this data, I then develop conceptual models for each period that visually depict the grand strategies the actors employed.

Third, I compare the collected data, identify the cases' similarities and differences, and draw conclusions on how international conflict has changed over time. To complete this step, I then analyze the role cyber technology played in the process by examining how the states modified their strategies to exploit the other's vulnerabilities through the new capability.

Taken together, these steps and their attending analytical frameworks and definitions provide the requisite structure for analyzing international conflict and the revolution in cyber technology. Although the topics are complex and multivariate, by applying rigorous methods, a solid theory, and clear definitions, this approach ensures the research meets the necessary empirical requirements. In the process, I demonstrate not only that international conflict has changed, but most significantly, how the revolution in cyber technology is affecting its evolution.

Chapter Three: The Revolution in Cyber Technology

Introduction

The revolution in cyber technology has had a global impact unlike any other invention in modern history. Widespread, rapidly evolving, and increasingly integrated into our daily lives, it has dramatically altered the way people conduct business, communicate, fight, and even fall in love. In the process, cyber technology has brought both promise and peril, and raised fundamental and unanswered questions about how it is changing power, politics, and social relations writ large.

One of the central questions scholars continue to wrestle with is how cyber technology has impacted international conflict. For some, cyber is the ultimate weapon, through which a covert attacker can undermine society and governance or even alter the foundations of the international system with minimal accountability (Clarke & Knake 2010; Kello 2017; Sanger 2018). For others, cyber is a limited tool that, while capable of creating important effects, must be supplemented by other weapons to have a substantive impact (Libicki 2011). Finally, there are scholars who argue that the claimed risks inherent in cyber conflict are overstated and based on a misunderstanding of the technology, its vulnerabilities, and the damage it can inflict (Gartzke 2013; Lindsay 2013).

Collectively, these scholars present a range of findings that, although insightful, are often driven by imprecise definitions, a focus on kinetic effects, and segmented approaches that fail to holistically analyze how actors are employing information systems to achieve their goals. In this chapter therefore, I will address these shortfalls by comprehensively exploring cyber technology and its impacts through a four-step process.

First, to understand the technology today, we must appreciate its history. As such, I will start with an overview of how cyber technology evolved from its invention until 2019. This analysis will use both qualitative and quantitative data to trace related technological developments forward in time from the internet's origins as a government collaboration tool to its nearly ubiquitous presence today.

With this historical background as a foundation, I will then discuss the degree to which cyber technology has become integrated into most societies and the changes this has brought to their physical infrastructure, economies, societies, and government. Third, I will evaluate the vulnerabilities this integration has created by connecting critical infrastructure, government services, and people's minds to an open architecture that is manipulated by actors who can be hard to detect, identify, and hold accountable. As part of this analysis, I will also examine how state actors are exploiting these vulnerabilities. Moreover, I will discuss the defensive measures individuals and organizations are taking to offset these dangers and the costs they impose.

Finally, I will analyze how these vulnerabilities and cyber exploitations impact each of the variables in the neoclassical realist framework used throughout this research. Taken together, these steps will provide a detailed, holistic picture of the revolution in cyber technology that will serve as the foundation for subsequent analysis of its impact on international conflict. Through this process, I will ensure that the conclusions I reach are founded on an empirically-based, comprehensive assessment of the technology's risks and benefits.

A History of Cyber Technology

As defined in Chapter One, cyber technology includes anything directly or indirectly connected to the internet, including those devices that are ostensibly isolated from it but employ connective computer technology. While this provides some indication of what cyberspace includes, the physical infrastructure is only one component. In addition to the wires, routers, devices, and other material aspects, cyberspace also contains virtual, governance, and social elements. Each of these interactive parts influences how cyberspace is structured, used, and operated, and therefore must be considered in the analysis. While space limitations prohibit a detailed discussion of each component, through the below history I will provide a general schematic of how they fit into the overall picture.

With cyber technology's ubiquity in modern society, it is easy to sees its development and integration as natural and inevitable processes (Naughton 2016: 6). However, the path cyberspace followed was complex and built upon a myriad of steps and decisions that could have dramatically changed it from what we have today. To understand the technology, its strengths and weaknesses, and the role it plays in international conflict, it is important to grasp why it is structured, operated, and managed the way it is.

As with any complicated history, there are numerous and often conflicting versions on how the internet developed, who was involved, and when and where seminal events occurred. However, accounts largely agree that, while the idea of making information globally available reaches back to the 1930s, it started to come to fruition only in the 1960s (Cailliau & Gillies 2012: 32). This was driven mainly by the US Department of Defense, which was interested in developing a distributed command and control network that could rapidly and securely share data across vast distances even if some of the nodes were destroyed (Lukasik 2011; Brand 2001).

In the 1960s, researches at MIT, the Advanced Research Projects Agency (ARPA), UK National Physical Laboratory, and RAND, devised a scheme in which digital information could be broken into “packets” so multiple people to use the same telephone wire simultaneously (Leiner, et. al. 2009; Roberts 1978: 1307). To create a network, the researchers developed a system of nodes, or minicomputers, that would act as “post offices” at system junctures, where they would briefly store the individual packets until determining the most efficient and rapid route for their further transmission (Roberts 1978, 1308; Boehm & Baran 1964: 1-3). If one part of the redundant network was delayed or damaged, then the node would send the packets along a different, functioning pathway.

Although tests of this “packet switching” design showed promising results, the existing network suffered from significant delays due to the limits of technology at the time (Baran 1964). In fact, the first message sent on the Advanced Research Projects Agency Network (ARPANET), in 1965 consisted of two letters, “lo,” after which the system crashed (Garber 2014). Overcoming this challenge required additional technology advancements which came about as multiple organizations and individuals worked in parallel in the United States, United Kingdom, and France.

In 1969 the next important step occurred when an Interface Message Processor (IMP) was installed in a network linking UCLA and Stanford (Roberts 1978: 1308). The IMP, which was the product of multiple organizations’ intellectual and financial efforts, served a critical function by overcoming incompatibility among different computers attempting to communicate with each other (Naughton 2016: 8). This development, along with software advances, and a transmission line capacity increase, supported network expansion to 111 computers by March 1977 (Roberts 1978: 1308). During this time, multiple other networks were created in Europe and the US, especially as packet switching became cheaper than traditional direct transmission technology (1308-1310). Email was also created in 1972 to facilitate researcher collaboration (Leiner, et. al. 2009).

As ARPA and other organizations involved in network development sought to connect their projects in the early 1970s, the IMP design proved too limiting, however (Naughton 2016: 9). To overcome this problem and create a "network of networks," two members of the newly established International Network Working Group (INWG), Bob Kahn and Vinton Cerf, created the idea of network gateway computers and an updated operating protocol (Haffner & Lyon 1996: 222-226). To lessen the burden on the network itself, and increase reliability of data transmissions, the design transferred responsibility for packet tracking and reconstruction from the IMPs to each end of the process (226-227).

In addition, after five years of collaboration and experimentation, the INWG created the joint Transmission Control Protocol and Internet Protocol, or TCP/IP, which managed the network traffic and provided a common language (235-237; Naughton 2016: 10). Finally, to allow the system to transmit the packets to the right location, researchers also created an address system (Abbate 1999: 128-129). Collectively, these developments not only allowed the new network to grow, but also set the foundation for the current open internet structure, which allows for interconnectivity among networks of any almost any design (Leiner, et. al. 2009: 24).

ARPANET's expansion and growing publicity created problems, however. Specifically, as an increasing number of universities sought to gain access to the restricted net and funding became more constrained during the post-Vietnam military draw down, ARPA needed another organization to take over management responsibilities. The National Science Foundation (NSF), which had funding and an interest its own network, accepted the charter (Hafner & Lyon 1996: 240-241). In 1979, NSF began working with universities on the Computer Science Research Network (CSNET), that would allow for collaboration among computer scientists from academia, the government, and private business (242). By 1986, the network had grown substantially, to include most computer science departments and other research organizations, which provided the requisite financial support through annual dues (243).

Developments in networking technology and computers also changed dramatically in the 1980s, as they decreased in size and cost, and therefore became more widely available (Naughton 2000: 184-185). This development created opportunities for the general population, which led to the first open source creation of a networking software and "store-and-forward messaging system" (185-186). These efforts, "MODEM" and the "Computer Bulletin Board System" (CBBS) respectively, when combined with the networking software "Fidonet," created a publicly generated and rapidly growing network available to anyone with a computer and technical knowledge (187). These developments set the foundation for the first mainstream collaboration platform, Compuserve, and the subsequent social media revolution (Shah 2016).

The final main technical components of the internet as we know it today came together in the early 1990s as Tim Berners-Lee of CERN laboratory developed the http protocol, Universal Resource Locator (URL), and an initial web browser, that incorporated the hypertext link (html) technology developed in the 1980s (Cailliau & Gillies 2012: 33). Each of these elements evolved and became more advanced as other researchers and private citizens worked to facilitate internet navigation and information location. In 1993, when CERN placed this collection of elements on the public domain, the web's open architecture and basic design were cemented into the system (Cailliau & Gillies 2012: 33; W3C 2019).

From a governance perspective, the internet went through significant changes as well. As the internet grew and became an increasingly important international domain, its oversight was transferred from ARPA to the nongovernmental Internet Society in 1992 (Cerf 1995). In addition, in 1998 NSF transferred the responsibility for managing the technical aspects, such as domain name registration and IP address allocation, to the newly established, US-based non-profit Internet Corporation for Assigned Names and Numbers (ICANN) (ICANN 2019). Throughout, however, the open concept idea was maintained, as reflected in the publicly generated "Request for Comment" (RFC) process that is used to develop standards for web operations as well as ICANN's multinational structure and approach (York 2019; ICANN 2019).

As cyber-related equipment became faster, smaller, and cheaper, the internet expanded rapidly. While in 1995 users represented only .78% of the world's population and were concentrated in North America and Western Europe, by 2000 the internet had spread to every inhabited continent and was being used by 6.74% of the globe (Murphy & Roser 2019). These advances set the foundation for the next leap forward: user content creation.

This step, often called Web 2.0, gave cyber actors the power to develop and share their own information, pictures, art, and other creations in ways previously impossible. Although user content creation had existed since the bulletin boards system of the 1980s, those sites were largely the domain of computer scientists and other technically proficient people (Shah 2016). Starting in the mid-1990s, however, philosophical and technical developments combined to make user content creation more accessible and attractive to others (Obar & Wildman 2015: 745-756). As a result, collaborative web application quickly grew in popularity and availability as people were drawn to the opportunity to communicate with others around the world and gain access to the global stage (Shah 2016). This accelerated even more rapidly with the public introduction of Facebook and Twitter in 2006 (Jenkins 2013: 60; Obar & Wildman 2015: 745).

Collectively these technical and social elements generated an explosion in online presence. From 412 million users in 2000, the internet grew to over 1 billion in 2005, and to nearly 2 billion in 2010 (Murphy & Roser 2019). As of January 2019, there were nearly 4.4 billion users active on the internet and 3.5 billion on social media (Statistica 2019b). The internet was also present in every country, with a 57% global penetration rate and an estimated $2.8 trillion in e-commerce activity (Kemp 2019; Statistica 2019g).

From its humble beginnings as a fragile, dual computer connection to a world-spanning network that touches every nation, the internet and associated cyber technology have grown at an exponential rate. As the above description makes evident, however, multiple variables played a role in shaping how the technology has become integrated into our daily lives, the vulnerabilities it poses, and the challenges it creates for states in their governance and interactions. Throughout the remainder of this chapter, I will explore each of these elements.

Cyber Integration

In 1983, when the internet was in still its infancy, an estimated 10% of adult Americans had personal computers in their home, 1.4% engaged in online activity, and 74% of the computer owners agreed that online banking and purchases would be problematic for budgetary reasons (Fox 2014). By 2017, however, 90% of Americans had at least one computer, smart phone, or similar device in their home, 72% conducted their banking online, and 96% made online purchases (Pew 2017; Statistica 2019d). Across the developed world, we have seen similar patterns, with users representing 76% of the Russian population, 54% in China, and 81% in the European Union (EU) in 2017 (World Bank 2019d).

This increased reliance on cyber technology for everyday functions has extended well beyond people's private lives, to include nearly every facet of today's functioning society. While cyber access and use are impacted by socioeconomic and political factors, and therefore are not consistent across the globe or within states, over the past forty years the technology has nonetheless directly or indirectly become a fundamental component of society for much of the world's population.

For many people, however, the prevalence of internet capable devices in our homes, businesses, vehicles, and public services raises both promises and risks that stir the imagination and trouble the mind. Adding to this perplexity is the discreet, complex, and chameleon-like nature of cyber technology, which makes it difficult to understand and is often invisible to the naked eye. Combined with a distrust of the businesses that create the devices, write the code, and manage the data, and deep-seated concerns about criminal, corporate, and government infringement on people's privacy and other rights, these attributes lead to significant misunderstandings and uncertainty about the role of cyber technology in society today.

To provide some clarity on the these and related issues, in this section I will evaluate the level of cyber technology's integration into states' physical infrastructure, economies, societies, and government. As part of this analysis, I will also examine how the integration has changed each of these aspects of the modern state. Through this process, I will set the foundation for the remainder of chapter, in which I will evaluate the associated vulnerabilities and how they are being exploited in the international struggle for power.

Physical Infrastructure

In 2019, it seems that nearly every device contains some type of cyber technology. Whether it is a personal item, such as a smart phone, passenger car, washing machine, or television, or a component in a large power generating station, today's equipment is increasingly internet capable.

This development, often called the Internet of Things (IoT), is an evolving framework that has grown and changed with advances in hardware and software technology. Initially conceptualized in the 1970s, the idea of "pervasive computing" became a reality only in the 1990s as the computer industry started integrating sensors capable of connecting to and transmitting data over the internet (Ibarra-Esquer, et. al 2017: 2). Due to continuing advances, including enhanced chip functionality, lower power requirements, increased storage capacity, and more capable wireless networks, the IoT has since grown dramatically and passed through multiple evolutionary stages (Adat & Gupta 2017: 423-424; Atzori, Iera, & Morabito 2016).

In addition to the IoT hardware is the virtual component that includes the software and data elements of the system. While the software drives the devices and provides the brain for its functionality, the data typically informs the primary purpose of the IoT as an information collection and analysis platform. These virtual and physical elements are joined together in four layers ranging from the user, through network gateways, across infrastructure components, to cloud-based data analytics (Kumar & Mallick 2018: 111; Malik, Dalal, & Solanki 2018: 123-124).

Collectively, the IoT serves multiple purposes, including automated and remote monitoring and control over complex machinery, increased efficiency, facilitated software updates, and feedback mechanisms for producers on the performance of their products. As a result of these benefits, and the associated changing market forces and technological advances, the IoT has expanded greatly over the past decade. From 2009 to 2019, the number of devices connected to the internet grew from 0.9 to 26.7 billion (Statistica 2019c; Statistica 2017). In the process, critical components of society's daily functions, including corporations' industrial control mechanisms, the electric power grid, hospital life support systems, and transportation infrastructure have all become connected to the internet in one way or another. Also, seemingly mundane devices, such as washing machines, light switches, hot water heaters, and passenger cars have all joined the IoT.

In many ways, this growing connectivity has had tremendous impacts on today's physical infrastructure. These developments have largely proven beneficial by allowing for distant sensing and manipulation of complex, dangerous, or isolated functions that no longer require a person's contact or presence. Moreover, businesses can remotely manipulate and update software and hardware functions and monitor equipment performance, which facilitates troubleshooting and lessens the need for costly and time-consuming travel for the owners or repairmen.

At the individual level, cyber technology has changed life in fundamental ways by making it possible to accomplish daily tasks online or through other cyber connections. For instance, cyber integration now allows people to watch and control their homes from a distance, track their physical fitness, and monitor their health through wearable devices or smart phones. People can also engage in online banking, pay bills, get directions, or complete a myriad of transactions from any location that has wireless connectivity or cellular service. In addition, the way people interact with cyber technology has increasingly shifted from personal computers to tablets, smart phones, voice assistance devices, game counsels, and virtual or augmented reality (Deloitte 2019; We Are Social 2018: 41). As a result, the number of connected devices has grown substantially over the past decade, with an average of 3.6 person globally and 13.4 per capita in North America (Cisco 2019).

Taken together therefore, the increased integration of cyber technology into the physical infrastructure has had many positive benefits. This, in turn, has created ever increasing demand for greater integration and associated efforts to make the technology smaller, faster, and more mobile. As a result, studies predict that the total number of devices connected to the internet will continue to expand, possibly reaching over 34 billion by 2025 (Lueth 2018). Whether these predications are accurate, or cyberspace will reach its technological, political, economic, or social limits, only time will tell.

The Economy

Cyber technology has had four substantive economic impacts. First, it has fundamentally changed the economies in most developed nations. In the US, for example, cyber technology has helped to drive a shift from heavy industry to an economy increasingly dominated by technology firms. This is aptly reflected in changes to the Fortune 500 top ten lists of the past forty years. Specifically, in 1980 the list was dominated by the automotive and petroleum industries, with only one technology company, IBM at number eight (*Fortune* 1980). The 2019 list, however, contains three technology-based companies and only one carmaker, General Motors, at number ten (*Fortune* 2019).

From a market capitalization perspective, the changes have been even more fundamental. For instance, for those 1980 top ten Fortune 500 companies that still exist in similar form and for which data is available, market capitalization increased by an average $11 billion dollars (7%) from 2006 to 2018.[1] During the same time, the five top valued US technology companies increased their market capitalization by an average of $603 billion (129%) (Macrotrends 2019).[2] These developments not only represent a change in the US economy, but also are reflected across the globe, as seven out of ten of the most valuable companies in 2018 were technology firms, with five being primarily internet-based (Statistica 2019j).

Second, while manufacturing businesses and "brick and mortar" stores still exist, and likely will continue to play a significant role in the market, there has been a fundamental shift in the character of economies as business models in the developed world have incorporated cyber technology and adjusted to market forces (Dennis 2018). This has played out in several ways, as companies have changed to meet growing e-commerce requirements and integrated technology into their "just-in-time" supply chains to maintain stocks at the requisite levels, decrease storage facility overhead, and adjust to rapidly evolving customer demands (Boyes 2015: 28). In addition, businesses have increasingly embedded technology into their production chains, which has decreased personnel costs and enhanced efficiency and precision, while also allowing for the

[1] Exxon, Ford, IBM, and General Electric.

[2] Facebook, Amazon, Apple, Microsoft, and Google / Alphabet

distribution of the manufacturing process across different regions to take advantage of lower labor costs and skills differential.

Moreover, the increased connectivity has led to the development of new economic sectors. For instance, the gaming industry has grown from a small segment of the economy to a highly profitable business that generated $134.9 billion in 2018, a 10% increase from the previous year (Batchelor 2018). Another newly developed economic area is the "sharing economy," which allows people to recover costs from underused or excess resources such as cars, homes, retail space, and workers through peer to peer transactions on web-based applications (Yaraghi & Ravi 2017: 3). Although the benefits are not equally shared across the world, in many locations the sharing economy has increased competition, lowered customer costs, and opened employment opportunities for people across the economic spectrum (9-10). As an indicator of the impact, some host companies, such as AirBnB and EBay, are routinely earning over a billion dollars in revenue per quarter (Somerville 2018; eBay 2019).

Third, as the internet and associated technology have proliferated, the amount of data has grown exponentially, from one billion gigabytes in 2005 to over twelve trillion in 2015 (Statistica 2019k). This pattern is continuing to accelerate, with 4.7 megabytes created every second in 2018 (DOMO 2019). In the process, data have become a new commodity that is collected, bought, and sold across the world, with associated revenue projected to exceed $189 billion in 2019 (IDC 2019). As a result, in 2019, data driven businesses like Google and Facebook have become highly valued companies that, along with device manufacturer Apple, the online shopping site Amazon, and the movie streaming service Netflix, have a collective market capitalization of $3.1 trillion (NASDAQ 2019).

In addition to data as a commodity, stored and mobile data such as personnel and financial records, shipment tracking, historical documents, and the myriad of other information components are of tremendous value to the companies producing them. While these records used to be maintained in paper form, as larger, more reliable, easily searchable, and sharable electronic storage capabilities have become available, records management has increasingly migrated to cyberspace. In the process, not only businesses' information but also people's medical, financial, and social records, have become digitized as well.

Society

Arguably, one of the greatest impacts created by the revolution in cyber technology has been the social component. Starting with email in the 1990s, internet connectivity has rapidly transformed how people communicate with each other. For instance, in 1980 60.1 billion pieces of first-class mail were sent in the United States. After peaking at 103.7 billion in 2001, however, that number dropped to 56.7 billion in 2018, despite a 32% population increase (US Census Bureau 1980; 2018; USPS 2019). At the same time, internet access increased from 52% of the population in 2000 to 89% in 2018 (Statistica 2019h).

Social media has played a substantial role in this process by changing how people stay in touch or establish new contacts. Starting with Classmates.com in 1995, social media has increasingly become a key platform for social interactions, with global users increasing from 1.5 billion in 2012, to 3.5 billion globally in 2019, representing 45% of the world population (We Are Social 2019: 7; 2012: 2). In the US, social media adoption has been even more substantial, growing from 50% to 69% of the population over the same time (Pew 2018b). This trend has also expanded to dating, job hunting, and social network development, as the internet has made it much easier to locate and connect with people of similar interests or needs (Rosenfeld & Thomas 2012).

As a result, social relationships have become more reliant on cyber technology. For instance, in 2004 nearly 93% of American households possessed a landline telephone, with less than 5% having a cellphone. By 2017, however, these numbers had changed dramatically, as nearly 55% of adults in the U.S. only used cellphones in their homes (Blumberg & Luke 2018: 1; Richter 2018). In the process, Americans have increasingly integrated smart phones into their daily lives, with 46% claiming they would be unable to live without one (Perrin 2017).

Globally, these trends have been largely mirrored as social media penetration in the Middle East and North Africa, China, and Russia reached 68, 60, and 66 percent respectively in 2018 (Poushter, Bishop, & Chwe 2018). Smart phone use has also expanded exponentially, although more so in developed countries. Specifically, the ownership rate in India is 24%, Mexico 52%, and Russia 59% (Taylor & Silver 2019). Similarly, within countries cyber technology has had differing impacts across wealth, age, and education demographics (Anderson, Perrin, Jian, & Kumar 2019).

Beyond social connections, cyber technology has also dramatically changed how people get and share information. This is particularly true of social media, which has greatly expanded potential sources of news and provided people with platforms on which to propagate ideas with no intermediary filtering mechanism (Allcott & Gentzkow 2017). As an indicator of its influence, in 2017 social media surpassed print as a source of news for US adults, and 93% obtained some of their news from an online platform (Pew 2018a; Shearer 2018).

In nations with more stringent press regulations, such as China and Russia, this shift has been even more dramatic as people have turned to social media to gain insights not available from the state-run press (Li 2018; Smyth & Oates 2015). While censorship programs and firewalls do impact people’s abilities to share information and opinions freely across borders and within countries, users have also become more adept as using technology and code words to work around such restrictions (Poell & Zeng 2014: 4; Rauchfleisch &Schafer 2015: 141). In the process, social media and the internet writ large have created domestic and international connective webs that have greatly facilitated the transfer of information and ideas across cultural, political, and physical borders.

Government

Much like the rest of society, governments have integrated cyber technology deeply into their services, bureaucracies, and security functions. Specifically, to increase their efficiency and reach, governments have adopted electronic programs that facilitate sharing information internally among departments and externally with citizens and businesses. These e-government programs include online registration renewals, tax filings, and records searches that enable people to avoid long waits at offices, while reducing personnel expenses, and providing for a more open government structure (United Nations 2019).

Due to these benefits, since 2001 the United Nations has been actively promoting e-government as a means of facilitating development (United Nations 2017: 5). In the process, the UN has created a database, the “E-Government Development Index (EGDI),” which measures each member state’s level of connectivity, online services, and the people’s ability to access and use what is offered (United Nations 2019c). According to the EGDI, the top three nations for e-government are Denmark, Australia, and the Republic of Korea, with South Sudan, Niger, and Somalia rated at the bottom of the chart. The United States is in 11th place, Russia 22nd, and China is 65th (United Nations 2018).

In addition, much like the business community, government organizations have also sought to gain efficiencies by increasingly embedding technology into their bureaucracies and functions. As such, with the proliferation of desk top computing and email in the 1990s, cyber systems became a central component of the government office space, with most of the nearly two million federal government employees in the US having access to at least one computer (Office of Personnel Management 2018: 5). The importance of cyber technology to the government is also reflected in its financial investments in information technology, which have consistently increased over the past eight years, reaching over $60 billion in 2017 (Government Accountability Office, hereinafter GAO 2016). This trend is also followed by state and local government offices and is mirrored in developed nations across the globe.

Cyber technology has also had a significant impact on the military, which has found multiple uses for it, including networked sensors to support intelligence collection and analysis, unmanned vehicles, smart weapons, navigation, and communications capabilities. Moreover, cyberspace has become its own operating domain, much like the land, sea, air, and space, with the US, Russia, China, and other states regularly using it to conduct espionage, sabotage, and influence operations.

Additionally, as military platforms have become more complex, cyber technology has increasingly played an important role in facilitating control systems, providing operator feedback, reducing manpower requirements, and ensuring functionality across a myriad of moving parts (GAO 2018: 13). As a result of these benefits, and the American tendency to favor technology in war, computer hardware and software have become increasingly embedded into the military's capabilities, which has created a growing reliance on cyber technology to support day to day operations (Harris 2014: 291-293).

Moreover, governments and the commercial industries that provide 90% of the critical services for society have also integrated cyber technology into their infrastructures. As a result, cyber components, such as supervisory control and data acquisition systems (SCADA), distributed control systems (DCS), and programmable logic controllers (PLCs) are now resident in every aspect of the critical infrastructure, including traffic management, energy generation and distribution, and air traffic control systems (Stouffer, et. al. 2015: 1). In addition, sensitive functions, such as voting, records keeping, and tax filing services have increasingly gone online.

Finally, the proliferation of cyber technology across society has changed government organizations and responsibilities as states have created new entities charged with managing and protecting the infrastructure, data, and people from crimes and other threats. In addition, agencies have changed as organizations assumed new responsibilities and divested archaic functions. As with the commercial sector, this has also had an impact on the workforce and educational systems, which have faced challenges adjusting to the new skills requirements.

Overall, the above provides an outline of how deeply cyber technology has become embedded in modern society and describes some of the changes this has created. At the same time, however, this only represents a momentary snapshot of a revolution that continues to move rapidly forward. For instance, we are now on the cusp of what some are calling "Web 3.0," a still evolving environment that amalgamates artificial intelligence, blockchains, cloud computing, virtual reality, and the Internet of Things (Pinto 2019; Castelluccio 2018; Steiner 2018).

Although questions remain on Web 3.0 functionality and user integration, it is evident cyber technology is rapidly evolving and likely will continue to do so well into the future. How these changes will impact our physical infrastructure, economies, societies, and governments remains to be seen. At the same time, however, to prepare for the future, we must understand the vulnerabilities the above developments have created. This will be the focus of the next section.

Cyber Vulnerabilities and Exploitation

For most people on earth today, cyber technology is a reality of life. Due to its high level of integration, the technology's physical, virtual, social, and governance components have become common threads that collectively form a fundamental aspect of 21st Century modernity. While these developments have brought tremendous benefits, the technology's ubiquity, complexity, and ever-changing nature, have also created risks for the cyber-connected systems and societies that rely upon them.

In this section, I will provide an overview of these challenges by first exploring the general vulnerabilities created by cyber technology's deep integration. Next, I will evaluate specific vulnerabilities in the physical, economic, social, and government sectors of the modern state. In the process, I will also provide examples of how actors are exploiting these weaknesses and the defensive measures public and private entities have adopted to offset them. Collectively, this section will convey a holistic understanding of the risks inherent in cyber technology's centrality in today's society.

General Vulnerabilities

Since cyber technology has become so deeply embedded in the modern state, some of its characteristics create widespread vulnerabilities. These interrelated features include cyber technology’s rapid evolution, limited intruder detection and attribution, and the failure of accountability mechanisms to keep pace. Taken together, these factors generate an environment of seemingly endless opportunities for actors with even rudimentary capabilities to produce dramatic effects with limited concern for negative repercussions. While the associated risks should not be overstated, they also must be understood and taken into consideration.

As discussed above, from its invention until 2019, cyber technology has rapidly changed from a fragile dual computer network to a complex web with an ever-increasing number of users and applications. Along the way, the underlying technology has evolved as processor speeds and capacity have dramatically increased while their physical dimensions have grown substantially smaller. Simultaneously, the software has changed as well, driven by technological advances and human ingenuity on how to use the technology in new ways. Whether measured by the exponential expansion in IoT devices, the proliferation of internet and social media users, or the fundamental economic developments that have occurred, cyber technology has both created and undergone dramatic changes over the past decade.

Due to these rapid advances, as well as inherent human error, purposeful design, and the complexity of the resulting system, cyber technology contains numerous known and unknown vulnerabilities. Although some scholars argue that these gaps can be controlled, and therefore cyberspace is a defensively dominant environment, most conclude that the domain favors offensive actions (Rinear 2015: 686-687; Singer & Friedman 2014). Considering the technology’s ever-expanding uses, locations, and characteristics, as well as its rapid changes, open architecture, and the fact that it is designed and run by people, exploitable gaps are inevitable. Thus, as demonstrated by the frequency and impact of cyber-based operations over the past decade, and the seemingly fruitless attempts by government, industry, and individuals to prevent them, it is evident that cyberspace is an offensively dominant domain.

One indicator of this situation is data from the Common Vulnerabilities Scoring System (CVSS), which is a program through which businesses and organizations report detected vulnerabilities in information technology software. The CVSS, which feeds the National Institute of Standards and Technology (NIST) managed National Vulnerabilities Database, provides detailed assessments of reported problems, including a qualitative evaluation of their severity. Collectively, these reports allow users of the systems to understand both the technical characteristics and associated risks of the weaknesses (NIST 2019b).

Over time, the CVSS has shown a marked increase in both the severity and the number of reported weaknesses. Specifically, in 2001 the total reported vulnerabilities were less than 2,000, while by 2018 they had exceeded 16,000, with over 4,000 considered of a high-risk nature (NIST 2019a; FIRST 2015). Although enhanced reporting and awareness likely contributed to these increases, the continuing proliferation of cyber technology and the inherent vulnerabilities embedded within it, have also undoubtedly played a significant role.

Closely associated with these challenges is the issue of detection. Due to cyber technology’s complexity, ubiquity, and networked structure, actors can hide their malign behaviors by blending into the everyday “noise” of internet activity. Thus, depending on the network’s defenses and the intruders’ actions, hackers and their tools can remain in the system undetected from minutes to years (Kello 2017: 69). During their time inside, these actors can siphon off critical information, install viruses, inflict damage, undermine processes, and monitor sensitive activities otherwise assumed to be private.

In addition, as the cyber technology industry has become more distributed virtually and physically, the risks of states or other actors using supply chain vulnerabilities to install "backdoor" access into the operating systems has become more of a concern (*The Economist* 2019: 16-17). While this intrusion vector is receiving more attention, it is difficult to detect and counter as it avoids many of the traditional security measures on which most people and organizations rely (Director of National Intelligence, hereinafter DNI 2017b).

Exacerbating these factors is the ever-changing nature and proliferation of the malicious codes cybercriminals use to penetrate, manipulate, exploit, and damage systems. This is aptly demonstrated by industry studies that have found a persistent increase in new malware detections per year, from 47 million in 2010 to 898 million in 2019, with an estimated 350,000 newly detected each day (AV-Test 2019). In the process of seeking online prey, cybercriminals have also created a new and fluid lexicon of threats, including cryptojacking (stealing cryptocurrency), ransomware (encrypting data for ransom), and formjacking (copying credit card data from online shopping sites), to name a few (Symantec 2019).

Moreover, once an intrusion has been detected, it still might take months before security professionals are able to remove an advanced virus, gain an understanding of what has been stolen or damaged, and return operations to normal. Even then, however, the malware may not be completely eliminated, as it can continue to propagate across the network, morph to offset security measures, or reactivate after a self-imposed dormant period (Fox-Brewster 2017;

Falliere, O Murchu, & Chien 2011). Collectively, this creates challenges for understanding the extent and true costs of a cyber intrusion. For some organizations, therefore, the damage may never be fully known or calculable due to intangible losses to their prestige, expended manhours, and downstream effects on time sensitive logistics chains (Council of Economic Advisors 2018: 6).

In addition, actor identification and accountability remain difficult. While cyber security experts are becoming more adept at attribution, at the same time malign actors are also learning to use false flags, commercially available capabilities, proxies, and other tools to avoid detection and identification (Symantec Corp. 2018; Rid & Buchanan 2015). Even if the actors are identified, however, it is unlikely they will be held accountable due to jurisdictional challenges, archaic laws, evidentiary limitations, and a lack of reporting (Grimes 2016).

Finally, the greatest vulnerability comes from the fact that most cyber systems are operated by humans. According to government and industry studies, over 90% of all intrusions are due to opportunities created by systems' users (Libicki 2015: 33; GAO 2017a). While much of this is the result of human error, laziness, or technical ignorance, some intrusions are due to purposeful acts by "insiders" who want to harm the organization, gain financially, or achieve a political goal. Of these inside actors, the most notorious is Edward Snowden who stole and then leaked 1.5 million sensitive government documents, causing extensive embarrassment and inflicting incalculable costs to US foreign policy and national security (US Congress 2016).

At the international level, these concerns are exacerbated by the amount of resources governments can invest in offensive cyber programs and the lack of a legal framework to guide their behaviors. While most scholars argue that international law applies in cyberspace, and therefore no legal vacuum exists, in practicality the current regime falls short in addressing some of the most fundamental concerns (Schmitt 2015; UN GGE 2013). In addition, the law is largely based on complex language extrapolated from pre-cyber era conventions and customs. Thus, at best, international law in cyberspace is a patchwork of archaic provisions, stretched into convoluted interpretations that only encourage malign behaviors (Hathaway 2017).

Physical Infrastructure

Of all the specific vulnerabilities, those resident in the states' physical infrastructure have gained the most attention from scholars and policy makers. Fears of a "cyber Pearl Harbor" in which an adversary uses information technology to shut down or destroy fundamental components of the nation's critical infrastructure have been widely discussed in the literature, press, and official documents. While maligned by some as an overstatement of cyberattacks' potential impacts, the threat is nonetheless real as a potential vector for strategic surprise against the United States and other advanced cyber-reliant societies (Goldman & Warner 2017).

These concerns are founded on the systems' interconnectedness, which presents the risk of direct and indirect cascading effects as the failure of one component can cause a chain reaction across the infrastructure, economies, and societies at the national and international levels (Critical 5 2015: 5; Murray & Grubesic 2007: 102). This is particularly true of the electrical grid, which is not only an indispensable resource for modern society, but also is at considerable risk because of its heavy reliance on vulnerable industrial control systems (NCCIC 2016: 4).

The vulnerabilities increase exponentially when applied across all sixteen categories of critical infrastructure identified by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (hereinafter CISA) (CISA 2019a). These interdependent categories, which include commercial, defense, manufacturing, and communications sectors, among others, represent systems of such importance that negatively impacting their functions would be debilitating to the nation's security, economy, and public health (White House 2013). However, embedded in the associated physical components are a plethora of information technology capabilities that, while important for monitoring and managing complex and interdependent systems, also contain both known and unknown vulnerabilities (Critical 5 2015: 7). As a result, the critical infrastructure inherently includes vectors of attack that, unless identified, secured and monitored, present a threat to the economic, social, and physical well-being of the countries that rely upon it.

The risks also extend beyond critical infrastructure to everyday elements of society, such as automobiles, medical devices, smart televisions, and all other devices in the IoT (Symantec 2106: 16-17). Unfortunately, due to the rapidity of IoT expansion, security measures have not kept pace, creating vulnerabilities in the devices and the associated systems (Department of Homeland Security 2016: 2). These vulnerabilities present an exploitation opportunity to not only disrupt the infected equipment, but they also provide external actors with access points into otherwise secure systems. In addition, billions of IoT devices also represent potential "zombies" that the malware can recruit into a botnet amalgamation to proliferate, conduct attacks, or execute surveillance activities (Graff 2017b; Tiirmaa-Klaar, et. al. 2013: 3).

Collectively, these individual vulnerabilities create potentially significant risks for states that rely upon the physical infrastructure to effectively govern. According to the US Department of Homeland Security, there are four critical functions for the government and private sector that, if interfered with would be debilitating. These include the ability to connect society through communications, distribute supplies and transport people, manage services and processes, and provide critical resources such as food, electricity, housing, and water (CISA 2019b). Unfortunately, these functions inherently rely upon the physical infrastructure, which means they are subject to risks created by the integration and proliferation of cyber technology into nearly every aspect of society.

These potential dangers have been aptly displayed by repeated Russia-based cyberattacks against Ukraine. For instance, on the night of December 23, 2015 Russian-linked hackers attacked three electricity providers in Kiev, cutting the power to approximately 225,000 people for three hours (Electricity Information Sharing and Analysis Center 2016: 1). These attacks were highly synchronized, in depth operations that not only severed electrical power, but also overwhelmed emergency call centers and communications nodes (4-5). In addition, using Ukraine as their testbed for military cyber operations, Russian attackers have interrupted banking, rail transportation, and other fundamental components of modern life (Greenberg 2017).

Ukraine, however, has not been the lone victim of state-sponsored cyberattacks. Rather, in 2018 alone dozens of states were subjected to cyber-based operations against their infrastructure, governments, and defense industries (Center for Strategic and International Studies, hereinafter CSIS 2019). While most were not at the same level as Ukraine's experiences, they nonetheless indicate that cyberspace is highly contested, and states' infrastructures are an open target. According to government and industry reports, the primary perpetrators include Russia, China, Iran, and North Korea, although attribution and accountability remain problematic (Davis, et. al. 2017).

The Economy

There are three significant economic vulnerabilities created by cyber technology in modern society. First, cyberattacks and data thefts can have significant negative impacts on economic stability and growth. While the methods for calculating losses vary widely depending on the costs included, definitions used, and timeframes evaluated, multiple studies indicate that illicit cyber activity worldwide inflicts damages ranging from tens of billions to trillions of dollars annually, and the numbers are increasing with time (Lewis 2018: 6-7).

In the United States, for example, government and industry reports show that in 2016 malicious cyber activity cost the economy between $57 and $109 billion and each reported cyberattack inflicted an average of $468 million in lost stock value for the target company (Council of Economic Advisors 2018). Thus, even without debilitating cyberattacks on critical infrastructures, actors are still inflicting significant losses. Should a major attack occur, however, the damages are likely to be exponentially higher, possibly creating another financial crisis on par with 2008 (Mee & Schuermann 2018).

Second, are the costs related to espionage and intellectual property theft. As with calculating economic losses due to cyberattacks, expenses incurred from these activities are difficult to calculate due to under reporting, their often-hidden nature, and the challenge of accounting for indirect costs. However, estimates range from $180 to $500 billion dollars annually, representing 1% to 3% of the US GDP (National Bureau of Asian Research 2017: 1-2). Considering that in 2013 intellectual property related industries contributed an estimated $6.9 trillion to the US economy and employed 39% of the nation's workforce, these thefts represent a significant economic risk (8).

Third are direct costs due to national and corporate investments in cybersecurity to protect against threats and meet regulatory requirements. For instance, in the US 2019 fiscal year budget, the White house requested $15 billion for cybersecurity-related expenses, which reflected a 4.1% increase over the previous year (White House 2018a: 273). Globally, governments, industry, and individuals collectively spent an estimated $151 billion on cyber security in 2018, a number which is expected to increase by at least 10% per year for the foreseeable future (Statistica 2019i).

Despite these investments, however, cyber-based attacks and espionage continue, with all measures indicating an increasing rate of occurrence. In the process, these vulnerabilities create significant risks to stock markets, financial institutions, industry, and the sharing economy, all of which are important to the economic well-being of most developed nations (Council on Foreign Relations 2018).

Society

Even though much of the literature and official attention has focused on the physical risks associated with cyber technology, the social component arguably presents a more insidious and potentially dangerous threat. Specifically, while physical damage can be repaired and the effects mitigated, social challenges are often more complex and difficult to detect, understand, and control. As such, the focus on the risk of a “cyber Pearl Harbor” ignores the more prevalent and subtle threats presented by actors’ efforts to manipulate society and gain a soft backdoor into states that are otherwise heavily invested in protecting their physical infrastructure. Since 90% of all network intrusions are connected to user-created opportunities, the social element in many ways is the lynchpin for all other components of the cyber vulnerability problem.

There are four aspects of this challenge that must be taken into consideration. First, is social engineering. Since all cyber technology involves some level of human interaction in the form of users, programmers, builders, or technical support, there is a close relationship between the systems and people who are inherently susceptible to direct or indirect manipulation. Through persuasion, threats, false familiarity, and other baiting techniques, therefore, malicious actors can leverage this connection to gain access to sensitive information, inject malware, or penetrate otherwise well protected systems.

Second, due to the high level of social media penetration globally, actors around the world have the ability to directly connect with large segments of the population in most developed countries. While these applications offer tremendous benefits in terms of social connectivity, due to their global proliferation and the funneling effect created by their underlying algorithms, social media platforms also provide a powerful venue for political, social, and criminal manipulation campaigns. In addition, since most people obtain some of their news online, they have ready access to information sources that lack the professional vetting processes and corporate accountability of traditional media. These features, plus the widespread availability of advanced graphics and digital design tools, allow malign actors to exploit people’s inherent biases by propagating highly convincing false stories, selective information releases, graphic videos, and other socially corrosive products. As we have seen in Europe and the United States, these operations can create severe effects by playing on people’s fears and aggravating political, racial, and other divisions.

Third, are the social tensions created by how the technology is used and controlled by corporate and government entities. Specifically, as reflected in recent Congressional hearings and related news stories, people are challenging companies' online data collection programs and how they are failing to protect the associated personal information while profiting from it (Steiner 2018). Closely related to this are government monitoring and intelligence collection operations, which raise questions about privacy, freedom of speech, and other human rights. While these programs can enhance state security, they also create tensions within society that, due to the propagation of valid or false information about their existence, can cause a backlash that undermines intelligence and law enforcement capabilities.

Finally, cyber technology's integration into the economy has had a direct impact on people's financial well-being. While new sectors, such as the sharing economy and information technology sectors have expanded opportunities for some, others have been displaced as automation has been adopted in the workplace. In areas with high levels of routine task-oriented employment, this has put pressure on workers in mid-level jobs, many of whom were replaced by automation and low-skilled, low pay positions (Muro, Maxim, & Whiton 2019: 26-28).

These forces have also exerted pressure on states' education and immigration systems, which have struggled to adjust. In addition, associated changes have often created or exacerbated political divisions due to differing perspectives on immigration and educational reform, and the feeling by segments of the population that they have been locked out of opportunities. Although not cyber vulnerabilities *per se*, these tensions nonetheless create opportunities for exploitation by actors who want to undermine a state's social fabric and internal stability.

Government

As the entity primarily responsible for maintaining security, state governments must not only address the individual and collective challenges created by the above vulnerabilities, but also must deal with those resident within their own structures as well as at the international level. Therefore, policymakers face a complex task of managing threats to the physical infrastructure, economy, and society, while simultaneously mitigating internal vulnerabilities and effectively responding to external stimuli.

A key component of how these vulnerabilities are addressed is the relationship between the government and private sector. As a tabletop exercise simulating an attack on the Baltimore electrical grid demonstrated, legal, regulatory, operational, and procedural challenges can hamper responses and recovery (Intelligence and National Security Alliance 2018: 2-3). Thus, bureaucratic processes and regulatory frameworks, as well as interorganizational trust, collaboration, and information sharing, play significant roles in how well governments perform their critical functions.

For instance, in the US, the Department of Homeland Security monitors and protects the nation's critical infrastructure, through CISA. For cybersecurity related issues, the National Cybersecurity and Communications Integration Center (NCCIC) is the lead organization. Together, these elements work with other government agencies, private entities, and the public to identify risks, protect the critical infrastructure, and respond to threats (CISA 2019c).

Although the NCCIC technically has the lead, however, there are numerous other departments, agencies, and private entities involved in defending the nation's critical infrastructure. Depending on the nature and source of a cyber exploitation, multiple organizations, including elements of the Departments of Defense, Treasury, and Energy, as well as other members of the Intelligence Community, local and federal law enforcement, state and tribal communities, and numerous businesses and interest groups could be involved. This combination creates a complicated morass of acronyms, differing priorities, and disparate missions and cultures that, when overlaid on the multifaceted nature of the commercial and private sectors generate severe challenges. Moreover, where an international actor is implicated, additional organizations and factors such as foreign jurisdictions, diplomatic concerns, and complex legal and regulatory constraints are added to the fray.

Further increasing the challenges, the government itself contains a myriad of cyber-based vulnerabilities. Considering that each of the nearly two million government employees has access to at least one computer, and the workers and leaders are subject to the same social engineering risks as others, the number of potential attack and influence vectors inside the US Government is vast (GAO 2017a; Office of Personnel Management 2018: 5). In addition, as the US military has increasingly integrated cyber technology into its weapons, communications, and surveillance platforms, the number of vulnerabilities to exploitation has correspondingly increased (GAO 2018). These challenges are not unique to the US Government, however, as every other developed country is subject to similar threats. Ironically, this creates a pattern in which, the more technologically advanced a society is, the greater its vulnerabilities to cyber-based attacks, crime, espionage, and social manipulation (Department of Homeland Security 2016; Clark & Knake 2010).

At the international level, these vulnerabilities and their exploitation by state actors have raised fundamental questions about how leaders should measure power (Eriksson 2007: 124). Specifically, with the advent of cyberspace, a new domain has been created involving capabilities that fall outside traditional military metrics and which are difficult to objectively measure, track, and manage (Inkster 2018; Venables, Shaikh, & Shuttleworth 2017). Moreover, as reflected above, this domain is not isolated from the rest of the state but is deeply integrated into it. As such, threats to its virtual, cognitive, or physical components will manifest in broader effects throughout states' economic, societal, infrastructure, and government elements. Adding to this complexity is cyber-based espionage, which, as demonstrated by China's massive intellectual property theft campaign, has risen to a new volume (US Senate 2016). This not only creates economic harm, but also provides the thieving country with the ability to more rapidly close technological gaps than previously possible.

Finally, due to the proliferation of false information, leaders are now faced with the challenge of discerning truth from fiction in their decision-making. While the Foreign Policy Executive (FPE) is typically backed by an array of professional intelligence analysts, regional specialists, and other advisors, every person in this chain is subject to human biases that make them vulnerable to disinformation and deception. In addition, the president and his close circle will likely have their own sources of information and will inevitably favor certain points of view. As such, rather than mitigating falsity, the bureaucratic process may actually reinforce it.

Defenses

Although cyberspace and its associated applications and devices contain numerous vulnerabilities, it is important to note that the domain is not an uncontested free for all. Rather, as mentioned above, states, businesses, and individuals are heavily invested in protecting their information technology. In addition to these financial expenditures, within the United States and other developed nations, there are numerous organizations dedicated to identifying, countering, and prosecuting cyber threats. As a result, while attribution and accountability present significant challenges, and most of the estimated one million daily cyberattacks are never prosecuted, actors are still largely prevented from inflicting significant damages due to firewalls, virus protection systems, personnel training, and organizational responses (Carbon Black 2019).

Moreover, as states have gained an understanding of cyber risks and improved forensics methods, they have begun to use other elements of national power to address the threats directly. For instance, in 2015 the US and China reached a partially successful agreement on controlling intellectual property theft, and the United States has imposed economic and political sanctions against Russia and some of its officials for their coercive actions in cyberspace (Segal 2016; Congressional Research Service 2019). The Department of Justice has also issued several indictments against cyber actors and has used diplomatic pressure to encourage other states to do the same (United States District Court Southern District of New York 2016). Thus, there is a growing realization of the multi-faceted threats resident within cyber technology and an increased willingness to act against them.

At the same time, however, these investments and actions are reactive, insufficient, and suffer from challenges with complexity, politics, resource limitations, archaic laws and the ever-changing nature of cyber technology. In many ways, therefore, the struggle to secure cyberspace is lagging those who are exploiting its vulnerabilities. The insufficiency of US efforts is aptly reflected in a 2018 report from the President’s National Security Telecommunications Advisory Committee, which argues that the current national cybersecurity trajectory is so dire that it requires a level of resource investments equivalent to the 1960s “moonshot” program (National Security Telecommunications Advisory Committee 2018). Considering the above challenges and that such a program has not been adopted, it is not a question of if there will be a cyber related crisis, but rather how and when it will manifest.

Conclusion

The revolution in cyber technology has ushered in dramatic changes, great promise, and growing risks. Over the past forty years, information systems have inundated every aspect life as people have integrated them into their physical infrastructures, economies, social relationships, and government functions. In the process, the technology has brought great benefits to each of these elements of the modern state.

At the same time, however, its deep integration has also created vast numbers of known and unknown vulnerabilities. While public and private organizations have attempted to offset these risks through hundreds of billions of dollars in annual investments and associated programs, processes, and regulations, the vulnerabilities and exploitation tools have continued to grow and change. As a result, state and non-state actors can use the domain to attack, manipulate, and steal from others with relative impunity and little fear of accountability.

Collectively, these challenges raise fundamental questions about international relations and the state of international conflict. Although the complex, multifactored nature of the problem makes it difficult to appreciate how the revolution in cyber technology is holistically affecting the modern state, by overlaying this paper’s neoclassical realist model on the vulnerabilities discussed above, it becomes clear that key components of the grand strategy formation process are exposed to attack and manipulation through the cyber domain (Table 1).

Table 1: Cyber-Related Vulnerabilities (Table 1)

Variables Vulnerabilities	FPE Perceptions	Ability to access & employ resources	Strategic Culture
Physical Infrastructure (attacks)	Confound stimuli. Create uncertainty on metrics & status of relative power positions.	Slow / complicate production, transportation, GPS, communications, & military capabilities.	Disrupt technology-centric way of war. Create uncertainty on its viability & operational art.
The Economy (attacks; manipulation; espionage)	Undermine real & perceived strengths. Shift economic balance of power.	Damage economy. Manipulate workers. Hinder supply chain. Destroy valuable data.	Deny financial resources required to implement strategy. Impose costs by forcing investments to offset risks.
Society (attacks; manipulation)	Aggravate domestic divisions. Increase threat axes, fear, & distrust.	Manipulate workers, security, & military. Divide & isolate the population & undermine support.	Exacerbate social divisions. Create fear. Raise questions on values & norms.
Government (attacks; manipulation; espionage)	Exacerbate internal divisions. Reinforce FPE biases. Create confusion. Raise questions on relative power.	Hinder bureaucracy. Recruit guerrillas & spies. Undermine elements of power.	Muddle assessments on strategic successes & failures. Inject false indicators.

Although cyber technology is not the only mechanism through which each of these vectors can be exploited or general effects achieved, its deep integration and extensive vulnerabilities allow actors to manipulate the variables in more direct, impactful, and widespread ways than ever before possible. Thus, this table demonstrates the irony that advances in cyber technology not only empower the states that embrace them, but also provide adversaries with additional attack vectors and more powerful ways through which to improve their tactical, operational, and strategic positions by directly and indirectly exploiting the target's physical, economic, social, and government components.

Based on the above, it is evident that actors' exploitation of cyber technology poses substantive risks to advanced states' security. At the same time, however, questions remain as to how these developments are impacting international conflict and what they portend. To analyze these questions, in the next chapters I will explore the grand strategies used by the United States and Russia during the Cold War (1980s) and the new era of conflict (2007-2019). I will then compare these strategies to identify the differences in the adversaries' approaches, why they changed, and the role cyber technology played in the process. Through these steps, I will test my hypothesis that the revolution in cyber technology is changing international conflict by enabling actors to directly impact states' grand strategy formation and execution processes in historically novel ways.

Chapter Four: The Cold War (1980s)

Introduction

From 1947 to 1990, the United States and the Soviet Union engaged in a global struggle for power that ebbed and flowed in severity, scale, and geographic range over time. Driven by domestic and international forces, as well as the personalities and beliefs of their respective leaders, the two powers vacillated along a spectrum of extremes that ranged from the promise of peaceful coexistence to the threat of mutually assured destruction. Along the way, the Cold War cost an unknown number of military and civilian lives as the US and USSR engaged in risky intelligence operations, bloody proxy wars, and periodic direct confrontations.

While the Cold War presents a complex puzzle that has generated a myriad of articles and books on its causes, conduct, and conclusion, for the purposes of this paper the primary point is to understand how the US and USSR engaged in the conflict and why they chose their respective approaches. In this chapter, therefore, I will explore the grand strategies the states adopted during the Cold War and the forces that drove their implementation. Considering the complexity of the topic and variations within it, I will focus on the 1980s. Although there were many segments in the conflict, in the 1980s leaders of the Soviet Union and United States struggled with policies that ranged across the conflict's spectrum and set the stage for its terminus. Thus, the case represents a microcosm of the Cold War and, as its last phase, the most recent example of the US and Russian struggle for power before the current conflict.

In this chapter, I will gain an in depth understanding of how the US and Russia have engaged in this New Era of Conflict by examining three main questions. First, what were Russia and the United States' grand strategic goals in relation to each other? Second, how did they employ their elements of national power to achieve these ends? And third, taken together, what do these approaches tell us about great power conflict in the 2007 – 2018 time period. Throughout, my central argument will be that, during this period of conflict, cyber technology played a fundamental role by providing the US and Russia with access and influence of a tremendous scope and reach. When coupled with their strategic approaches and demonstrated affinity for economic and information elements of power, respectively, this development and its effects raise fundamental questions about the character of conflict and the meaning of power.

To conduct this analysis, I will follow a four-step process. First, I will set a foundation for the chapter by briefly reviewing the relevant events and circumstances of the 1970s and describing the international stimuli of the 1980s. Second, to establish a baseline for the subsequent analysis, I will provide an overview of the grand strategies that the US and Soviet Union adopted during the decade. Third, as described in Chapter 1, I will use the neoclassical realist framework to conduct a detailed analysis of how the states applied their elements of national power to manipulate the adversary's decision-making and implementation processes.

Finally, I will compare the US and Soviet models to identify commonalities in their ways, means, and ends. This approach will allow me to develop a comprehensive model of international conflict in the 1980s and to determine the role technological, economic, and other factors played. Collectively, these steps will provide a solid foundation for comparison of the Cold War with the New Era of Conflict in the last chapter.

Historical Setting: the 1970s

As with any historical period, in many ways the 1980s were the product of the events that preceded them. Over the course of the three decades since the Cold War had begun, the world had experienced tremendous changes as leaders came and went, social norms evolved, technologies developed, and economic conditions improved and degenerated. In addition, while the US and USSR dominated the globe throughout the conflict, multiple other state and non-state actors played crucial roles as they were subsumed into the struggle as willing or unwilling participants or otherwise affected its progression through their actions.

Although each of the previous decades had an impact on the Cold War's progression, the 1970s played a key role in setting the stage for its ultimate outcome. For both the US and USSR, and most of the world, the 1970s were tumultuous times. From a global perspective, the era began in the throes of revolutionary struggles across much of the developing world. These wars, which were often cast in terms of proxy fights among the great powers, were typically founded in local grievances, with echoes of anti-colonialism set against their former masters and the elites they continued to support. Thus, throughout the decade such wars raged in Central and South America, Africa, and Asia, with the embers kept alight by external investments of people, weapons, training, and finances by the US, USSR, and their allies.

For the United States, the main conflict was Vietnam. While the US had been involved in the country since the end of World War II, in 1965 it started dramatically increasing the number of forces deployed to the country, peaking at over a half million in 1968. (United States Department of Defense. Defense Manpower Data Center 1968, hereinafter DMDC). Although the US had started a slow drawdown that year in response to popular and congressional resistance, by 1970 it still had 400,000 forces in the country and had lost nearly 49,000 soldiers' lives in a war that was proving to be unsuccessful and counterproductive (DMDC 1970; US Department of Defense, hereinafter DOD 2008).

At the same time, domestic unrest was growing, as antiwar sentiment, combined with economic and racial tensions, threatened the nation's social and political fabric. Driven by these factors, the US negotiated a peace agreement with the North Vietnamese government and quickly withdrew in 1973. Within two years, however, South Vietnam fell to a Soviet equipped onslaught from the North as the US conducted a panic-driven evacuation of the remaining Americans. Defeated in a major conflict for the first time, and suffering from extensive disciplinary problems, the military underwent a dramatic drawdown, losing 43% of its strength from 1968 to 1979 (DMDC 1968, 1979).

Moreover, the United States had also entered a period of economic malaise marked by rampant inflation and unemployment. Although the causes are contentious, several factors, including the collapse of the Bretton Woods system, harmful government policies, and an oil embargo imposed by Arab states, combined to create an enduring period of "stagflation" throughout the West (Barsky & Kilian 2001; Helliwell 1988). As a result, from 1971 to 1980, inflation in the US increased from 6.2% to 12.4% and unemployment expanded from 3.9% to 7.2% (Bureau of Labor Statistics 2019).

Adding to these problems was the Watergate scandal which resulted in President Nixon's resignation in 1974, further eroding popular trust in the US Government. Although subsequent presidents attempted to repair the nation's wounds, economic, social, and foreign policy problems persisted as the US struggled to reestablish itself at home and abroad. Seemingly emblematic of the era was the 1979 seizure of the US embassy in Iran, in which over 50 Americans were taken hostage and held for 444 days. Exacerbating the United States' apparent ineptness, an attempted rescue operation ended in disaster, with eight servicemembers killed when their aircraft collided in the desert. Thus, by 1980, with its social fabric under stress, military internally corroded, international reputation greatly damaged, and economy stagnated, the US appeared to be in a period of perpetual decline.

For the Soviet Union, however, the 1970s was a period of both peril and promise. Although the Soviet economy continued a slowing trend that had begun in the 1960s, the dramatic rise in oil prices combined with expanded petroleum production increased revenues by over 2000% (Trachtenberg 2018: 82; Zubok 2009: 249). In addition, the Soviets' uncontested invasion of Czechoslovakia in 1968 led to a perception that they had broad latitude in international affairs as their power and prestige had reached an apparent high point (Zubok 2009: 209).

At the same time, the Soviet leadership became increasingly concerned about the perceived threats posed by China and capitalist expansion. In response, they stepped away from détente while expanding efforts to enhance their military power and build an expanded communist support network (Ball 1998: 180). As a result, Soviet defense outlays increased significantly, growing over 35% during the decade (Ball 1998, 180; Swain, 1990: 105).

Finally, in direct contrast to the US withdrawal from Vietnam, in late 1979 the Soviets invaded Afghanistan to overthrow the existing government and counter the rising insurgency. Although the invasion generated a significant international backlash and soon became a costly quagmire from which the Soviets withdrew a decade later, at the time it appeared to be a successful demonstration of the Soviet Union’s ability to rapidly mobilize and deploy a large military force outside its borders (Collins 1980: 52). Thus, flush with a perceived military victory and renewed prestige, the USSR entered the 1980s with a sense of confidence tempered by economic concerns and perceptions of near and distant threats.

By the end of the decade, therefore, the Soviet Union seemed to have gained the upper hand as the superpowers entered a “new Cold War” driven by internal and external factors over which they had limited control (Brands 2014: 103). In the process, détente fell apart as distrust increased and the leaders of both states concluded that continuing the policy of coexistence was not in their nations’ best interests.

Thus, entering the 1980s, the stage was set for a revitalized conflict dominated by dramatic change and intense uncertainty as the United States and Soviet Union engaged in nuclear brinkmanship, productive negotiations, and an enduring competition that ended with the latter’s dissolution. Although the cause of the Cold War’s outcome is an enduring and controversial question, it is not the focus of this research. Rather, in the below analysis I will explore how the US and USSR struggled for power in the 1980s, why they selected their respective grand strategies, and what this tells us about international conflict at the time.

The 1980s: International Stimuli (Means)

As discussed in the first chapter, international stimuli include multiple elements, such as military and economic capabilities, geography, technology, and informational factors. Thus, the elements of national power are not limited solely to material metrics or even those over which the states necessarily have control. Rather, they include both measurable and intangible aspects that create the overall input that is filtered through the intervening variables in the grand strategy formation process (Ripsman, et. al. 2016: 34-38).

From the military perspective, when Ronald Reagan was elected in 1980 US forces were near their lowest numbers since before the Korean War (DMDC 1950, 1980). In addition, while the military had started to grow in 1979, it was widely considered to be a "hollow force" that, although seemingly capable on the surface, nonetheless faced critical shortfalls in qualified personnel, training, and equipment (Feickert & Daggett 2012: 2-8).

The Soviet Union, however, appeared to be reaching a tenuous pinnacle of strength, as it numerically outmatched the US in many categories, including nuclear missiles, military personnel, armor, aircraft, air defense systems, and submarines (Collins & Severns 1981). This apparent advantage extended to the NATO and Warsaw Pact alliances and was buttressed by the latter's standardization of equipment, which the US-led partnership had not adopted (107-117; Dunbabin 1994: 151 n. 3).

In addition, throughout the 1970s and early 80s, the Soviet Union had greatly expanded its collective security system to create a network of eighteen states across Africa, the Middle East, and South, Southeast, and Central Asia (Miyoshi 1987: 24-28). Added to the Warsaw Pact alliance, its long-standing relationship with Cuba, and proxy campaigns in the Caribbean, Central and South America, this network provided the USSR with extensive global reach (U.S. Department of State 1981: 11-12). While these developments were partially offset by the United States' increased international assertiveness, improved relations with China, and security assistance programs in many of the same regions, they nonetheless created the impression that the Soviets were expanding their footprint (Brinkley 2007: 1-4).

From an economic perspective, the US was still suffering from the malaise of the 1970s as its GDP grew 2.5% in 1981 then dipped into a recession before starting a general expansion the next year (World Bank 2019b). At the same time, however, the Soviet economic picture became increasingly negative in both relative and real terms as its productivity, consumption, and quality of goods proved inadequate to compete on the international market in most areas other than crude oil (Central Intelligence Agency, hereinafter CIA 1985a). Although analysts differ on the rate and causes of the collapse, both official Soviet and academic data indicate that, after a peak in mid-century, the economy began a broad-based decline that accelerated throughout the 1980s (Easterly & Fischer 1994).

Moreover, the US held superior positions in geography and information. Protected by two oceans, possessing numerous unrestricted ports of access in the east and west, bordered by friendly states to the north and south, and containing a large territory with vast resources, the United States enjoyed strong geographic security. In addition, the US held multiple overseas territories and bases that greatly expanded its global footprint. While the invention of intercontinental and submarine launched ballistic missiles had reduced the homeland's protective enclave to a degree, geography nonetheless provided relative safety from other forms of attack.

The Soviet Union, on the other hand, had only two ports that did not freeze in the winter and none that were unconstrained by maritime chokepoints. In addition, collectively the USSR bordered thirteen non-Soviet countries, including its adversary, China, and unstable states such as Iran and Afghanistan. The Soviet Union' periphery, therefore, presented significant security challenges and historical vulnerabilities that helped feed Russia's perceptions of insecurity. This was exacerbated by the fact that the USSR was composed of fifteen semi-autonomous states that, while ostensibly integrated into a centrally managed system, nonetheless maintained local identities and bureaucracies that undercut control and cohesion over time (Suesse 2017: 2936-2938).

From an information perspective, US values on human rights, individual freedom, and open markets held a greater attraction for people around the world. As one indicator of their respective reputations, during the 1980s the US gained 5.7 million immigrants while over 350,000 people emigrated from the Soviet Union despite severe constraints on the practice for most of the decade (Radford & Noe-Bustamante 2019; Heitman 1991). In addition, as the titular leader of the free world the US had strong influence in the international monetary system, and it dominated cultural and informational venues such as Hollywood and the news media. Finally, despite the Soviet Union's apparent technological competitiveness earlier in the Cold War, by the 1980s it had fallen far behind the United States in innovation and modernization (Chan 2015: 1-2). Thus, even though the United States faced some challenges, it still held dominating geographical, informational, and technical positions.

Collectively, these strengths provided the foundation for rebuilding US power over the next decade. As a result, despite the unfavorable economic circumstances of the 1970s and early 80s, throughout Reagan's time in office the US economy grew an average of 2.5% annually, with six years averaging over 4.5% (World Bank 2019b). At the same time, inflation dropped to 3.5% after a spike of 9.4% in 1981 (World Bank 2019e). Similarly, the military grew by over 100,000 personnel, while its quality and capabilities improved dramatically (DMDC 1988). By the end of the Reagan administration, therefore, the US had overcome every shortfall and was set for an era of tremendous growth and power.

The Soviet Union, on the other hand, was suffering a dramatic economic decline that it attempted to reverse by boosting production through defense cuts and resource reallocations to civilian purposes (World Bank 1990: 9). However, target rates were rarely met, and defense outlays likely increased in relative terms throughout the 1980s (Allen 2001, 867-868; Steinberg 1992; International Monetary Fund 1990, 7-9). These challenges were exacerbated by a substantial drop in crude oil prices in 1986, which, due to the Soviet Union's increased reliance on oil exports for hard currency, created an additional negative effect on its economy (Statistica 2019a; Ermolaev 2017).

Moreover, despite substantial defense spending and the USSR's ostensible military superiority in most categories early in the decade, by 1990 the Soviet and Warsaw Pact militaries were technologically inferior to the US and North Atlantic Treaty Organization (NATO) in most systems and they faced increasing personnel problems due to unpopular draft policies (United States Department of Defense 1990: 46-74). At the same time, the Soviets suffered an ignominious defeat in Afghanistan, losing nearly 14,000 soldiers and large amounts of equipment to the US supported mujahedeen (Cassidy 2003). Overall, as the decade wore on, fractures within the Soviet system grew as separatist movements within some satellite republics gained power and central economic and political control mechanisms broke down (Suesse 2001: 2938-2939). In comparison, NATO became more unified, particularly after the Soviet failure to divide the alliance over the Pershing II deployment to Europe, which, despite some popular protests, was nonetheless implemented with support by member states (Nuechterlein 1990).

Thus, for the US and Soviet Union, the international stimuli for the 1980s were an evolving set of conditions that, as time passed, became increasingly favorable to the former in all metrics of power. Along the way, both states adopted grand strategies designed to adjust to and shape these circumstances, with varying degrees of success. In the subsequent paragraphs, I will outline these strategies and followed by a detailed examination of how each state attempted to employ their instruments of national power to manipulate the opponent's decision-making and implementation processes.

US Grand Strategy in the 1980s

An Overview

During the Cold War, the US famously adopted a containment strategy. Drawn from George Kennan's "X Telegram," the approach was based on his theory that the Soviet Union was inherently expansionist and internally weak and therefore could eventually be defeated if held in check wherever it sought to create client states (Keenan 1947). Although the US followed this strategy in a general sense throughout the Cold War, the ways, means, and ends varied significantly as administrations adjusted to differences in their perspectives as well as domestic and international conditions. Thus, each president employed a variation of the approach that, to be understood, must be analyzed in individual detail.

For Ronald Reagan, scholars continue to debate whether he had a grand strategy, what it included, and whether it was successful. According to some, Reagan was a clear-eyed strategist who understood the Soviet Union's inherent weaknesses and worked diligently to exploit them (D'Souza 2003; Meese 1992). Others, however, argue that the President was a poor leader who lacked a consistent vision. Thus, any successes were more the product of timing than effective policies (Wilson 2007).

Unfortunately, these analyses are often based on selective evidence and fail to account for external developments, inconsistencies in the administration’s approach, and changes in its policies over time (Fischer 2010). A more objective examination, however, demonstrates that, while US policies in the 1980s were disjointed at times, Reagan did have an enduring vision that manifested in a consistent, although evolving, grand strategy. To demonstrate this and to understand the US approach, in the next sections I will examine the Reagan administration’s goals and the ways it sought to achieve them.

Ends

During Reagan’s terms in office he routinely issued National Security Decision Directives (NSDD) as a mechanism for guiding the administration’s actions and statements. These NSDDs were the end product a complex national security decision-making process, which involved the main elements of the bureaucracy. Although the NSDDs were not necessarily implemented as the President directed, they are nonetheless an apt reflection of the Foreign Policy Executive’s collective goals and preferred method of conflict. Therefore, they form the foundation for the below analysis of US goals in the 1980s.

When Reagan was first elected, the administration’s primary objectives were to reverse the perceived decline in US power and to use the enhanced position to deter the Soviet Union from attacking its interests while gaining agreements on nuclear weapons and other critical areas of disagreement (White House 1982i; White House 1982f; White House 1983h). During this rebuilding process, the administration also worked to contain and reverse Soviet expansion, pressure it to undergo internal reforms, and to reduce nuclear weapon stockpiles (White House 1982i; White House 1982f; White House 1983h). Finally, the US sought to eliminate Soviet influence in Europe, Latin America, and Africa while enhancing US relations with key states (White House 1982e; White House 1982a; White House 1983e; White House 1983d; White House 1983b).

Although this initial strategy was largely reactive in nature, by 1984 the NSDDs reflect a growing sense that the US was in a position of relative strength (White House 1984a). Thus, while the Soviets continued to be the primary threat to US interests, the administration sought to exploit perceived opportunities to shape the global environment, encourage internal reforms in the Soviet Union, and assume the upper hand in negotiations (White House 1986c). By 1988 this perception of success had grown considerably, as the US strategy appeared to be bearing positive results (White House 1998c). At this stage, therefore, the administration became more conservative, as it sought to consolidate gains and achieve more reforms and openness on the part of the Soviet Union (White House1988b).

Taken together, these NSDDs demonstrate that, during the 1980s, the US pursued a global grand strategy with four main objectives vis-á-vis the Soviet Union. First, it sought to deter the USSR from attacking the US or its interests. Although the primary focus was on preventing nuclear war, the FPE was also concerned about a conventional conflict in Western Europe. Second, from the beginning of his time in office, Reagan was personally interested in reducing the states' nuclear weapons stockpiles. Not only was this necessary from a balance of power perspective, but it was evident to him and others in the administration that the weapons posed excessive risks, particularly in the context of the times. Third, the administration attempted to reverse Soviet enlargement and to prevent further expansion. This was particularly true of Latin America, which was a high priority concern. Finally, the US sought to induce favorable changes within the Soviet system, especially related to its repressive domestic policies and destabilizing behaviors abroad.

Whether this strategy was successful, and the administration deserves credit for bringing the Cold War to a positive close, is beyond the scope of this analysis. However, as reflected above, during the 1980s, the US did generally follow a grand strategic vision that evolved with international and domestic circumstances. In the next section, I will examine the ways the administration attempted to achieve these ends by analyzing how it employed the nation's elements of national power to achieve its goals.

Ways

As outlined above, in the 1980s the US had a growing set of means available for use in achieving its grand strategic ends. While these means were often applied in disjointed, wasteful, and questionable ways, collectively the methods used demonstrate how the US engaged in international conflict in the latter stage of the Cold War. Thus, by examining how the US applied its elements of national power to achieve its goals, we can understand its model of conflict during that time.

Deterrence

Throughout Reagan's time in office, the US relied heavily upon its military resources to deter Soviet attacks on the nation and its interests. In doing so, the administration assumed the Soviets were rational actors who engaged in a cost-benefit analysis in their strategic decision-making. As a result, the US attempted to use the threat of force to convince Soviet leaders that any attacks would result in excessive losses (White House 1983h; White House 1986c). This calculus is apparent in the NSDDs and associated efforts in which the administration sought to close the perceived gap in Soviet military superiority by developing and fielding advanced nuclear and conventional forces (White House 1982c; White House 1986e). As a result, in the administration’s first five years, US defense outlays grew by 88%, from $158 to $253 billion, with military expenditures collectively increasing by 127% over the entire eight years (Congressional Budget Office 2014: 162).

In addition, the US employed technical, economic, and information capabilities to influence Soviet behaviors and perceptions. Specifically, the US used its information power to strengthen relationships with Western allies and overcome resistance to the deployment of intermediate range missiles to Europe (White House 1983f). Reagan also frequently used speeches to convey US ideas, shape Soviet perceptions, and influence domestic and foreign audiences (Reagan 1985). At the same time, the US invested heavily in building its nuclear arsenal and defenses so Soviet planners would recognize that the cost benefit analysis was not in their favor. This included antiballistic missile capabilities, a new class of mobile missiles, improvements to other strike systems and civil defense (White House 1986e; White House 1986c; White House 1986a).

Reducing nuclear stockpiles

Closely associated with deterrence was the administration’s goal to reduce the risk of nuclear war through verifiable reductions in the weapons and associated systems. To achieve this, the US used its military, economic, technical, and informational elements of national power to pressure the Soviet Union into negotiating and implementing agreements that would substantially lessen the numbers of missiles and warheads in the nations’ arsenals. Thus, the expansion of nuclear and conventional forces was not only designed to deter Soviet attacks, but the administration also wanted to create an incentive to bargain. This was reflected in the controversial MX (Peacekeeper) missile program, as well as the deployment of Pershing II missiles to Europe, which the administration used as a bargaining tool to achieve Soviet concessions on their intermediate nuclear forces (White House 1982c; White House 1983f). To support this goal, the US also enhanced its conventional capabilities, which allowed it to reduce reliance on nuclear weapons (White House 1986c).

In addition, the US invested heavily into research on the Strategic Defense Initiative (SDI), a space-based system that supporters argued could ultimately reduce or even eliminate the threat of nuclear ballistic missiles (Strategic Defense Initiative 1985: 8). From Reagan's perspective, the SDI program had two purposes. First, it would allow the US to reestablish the deterrent value of nuclear weapons that it perceived had been undercut by Soviet investments in offensive and defensive capabilities (White House 1985c). Second, Reagan believed SDI could generate a new deterrence calculus to replace the anachronistic policy of mutually assured destruction, thereby creating an incentive for the Soviet Union to negotiate reductions (White House 1983a: 3).

From an information perspective, the US attempted to use strategic communications to pressure the Soviet Union to alter its behaviors. Specifically, the administration sought to use public announcements to show how the Soviets were non-compliant with their treaty obligations while demonstrating that the US was willing to negotiate and act in good faith (White House 1985d: 10; White House 1986b; White House 1987b). At the same time, the administration wanted to build relationships with the Soviet leadership, an approach that became increasingly promising after Gorbachev assumed position as General Secretary in 1985 (White House 1985a).

As part of this, the administration publicly dismantled some capabilities to demonstrate US commitments to treaty obligations and to build trust (White House 1986e).

Reversing expansion

Of the goals sought, the administration arguably focused most heavily on pushing back perceived Soviet expansionism across the globe. This was particularly true of Latin America, which was a priority concern due to its geographical proximity to the United States and importance as a historical area of US influence.

To achieve its goals there, the administration used every element of national power to blunt Soviet incursions while also strengthening US ties to the region. For instance, Reagan issued stern warnings against Soviet and Cuban incursions into Central and South America, deployed forces to El Salvador and Honduras, conducted exchange programs, and provided economic assistance to friendly countries in the region (White House 1982a; White House 1983g; White House 1984c). As a result, from 1979 to 1986 US economic and military assistance to Latin America increased over 130% from $1.3 to nearly $3 billion (US Administration for International Development, hereinafter USAID 2017). Finally, Reagan ordered the Department of Defense to develop contingency plans for military action in Central America and used force in Grenada to remove the government, which had close ties with Cuba and the Soviet Union (White House 1982d; White House 1983b).

Latin America, however, was not the only effort, as the US also attempted to reverse Soviet influence in other regions. To this end, it used long-term associations based on trade, international organizations, and cultural connections to build and sustain relationships (White House 1982a; White House 1986c). In the process, the administration provided economic and security assistance to states in Europe, the Horn of Africa, South Asia, and other developing regions to foster growth and free market economies, which it viewed as critical tools in the fight against Soviet influence (White House 1982e; White House 1986c: 15). This also included aid to Pakistan and Afghan resistance fighters to pressure the Soviets into permanent withdrawal (White House 1987a).

Beyond military and economic tools, the US relied heavily on the information element of national power to increase US influence and undermine the Soviets. For instance, after the Soviet Union shot down a civilian airliner in 1983, the administration used diplomacy to sustain attention on the tragedy, offset Soviet counter-propaganda efforts, and pressure Asian countries to support the US (White House 1983c). Reagan also increased investment in radio broadcasting services, such as Voice of America (global), Radio Martí (Cuba), and Radio in the American Sector (Berlin), and he ordered the use of propaganda campaigns in Europe, Mexico, Venezuela, Columbia, and other Latin American countries (White House 1984c; White House 1982).

In addition, the administration used international forums to increase US credibility while highlighting USSR and satellite countries' violations of international norms, exposing their perceived hypocrisy, and preventing their messages from gaining traction (White House 1982f; White House 1983h; White House 1984b). Finally, it used the US Information Agency, exchange programs with the Soviets, and a visit to Moscow as opportunities to expose the population to the realities of their system and the United States' (White House 1986d; White House 1987a). Throughout, the US argued that it shared and supported the common ideas of mankind, ideals which the Soviet Union ostensibly sought to destroy.

Encouraging positive changes

Finally, the administration sought to coerce and encourage the Soviet Union to change its system and behaviors in a way favorable to US interests. Toward these ends, it used economic and technological tools. These included sanctions on the export of oil and gas equipment to the Soviet Union due repressive policies in Poland, rewards for economic liberalization in Eastern European countries, attempts to exacerbate inherent tensions in the Soviet economy, and “calibrated” rewards or punishments (White House 1983h; White House 1982h; White House 1982f). Reagan also sought to build free market relationships with other nations to prevent them from helping the Soviet Union overcome its economic problems (White House 1986c).

Technologically, the US restricted the transfer of defense and other sensitive knowledge to Eastern bloc countries, although it also increased scientific exchanges in the response to liberalizing policies (White House 1982b; White House 1982f; White House 1985b). In addition, Reagan attempted to use advances in technology to exert pressure on Soviet defenses and investments, while restricting exports that could help them overcome deficiencies (White House 1986c; White House 1988a).

Finally, as with the administration’s efforts to reverse Soviet expansion, it also employed radio stations, print media, cultural exchanges, and high-level visits to Eastern European countries as mechanisms for reaching Soviet and satellites populations and influencing the governments’ behaviors (White House 1982g; White House 1982f; White House 1984b). For example, Reagan directed that his 1988 Moscow visit should be used to communicate directly with the Soviet people, to encourage democratic reforms, protect human rights, and increase their understanding of US capabilities and policies (White House 1988c). Finally, the administration used international forums to undermine USSR credibility by highlighting violations of international norms (White House 1982f; White House 1983h).

Analysis of US Grand Strategy

The above demonstrates that the US had an enduring, although evolving, grand strategy throughout the 1980s and that it used every element of national power to execute it. To develop a model of the US approach to international conflict during the decade, in this section I will use conclusions from the above analysis on US grand strategy as the foundation for evaluating how it employed the state's means to influence each of the Soviet Union's neoclassical realist vulnerabilities. The results are reflected in Table 2, below.

Table 2: US Approach to International Conflict

Variables Elements	FPE Perceptions	Ability to access & employ resources	Strategic Culture
Military (nuclear & conventional forces, security assistance)	Field more capable nuclear & conventional forces to undermine Soviet confidence & deter actions. Deploy Forces to Latin America & Europe to deter Soviets, challenge access & use.	Induce Soviets to continue heavy investments in military capabilities to the detriment of other needs. Stress the Soviet economic system. Deny Soviets intelligence on US actions and intentions.	Conventional & nuclear enhancements & deployments to impact cost-benefit calculus in favor of US goals (deterrence, arms reductions). Espionage to understand, offset, & exploit Soviet strategic plans & operations.
Economic (aid, trade, export controls, sanctions, rewards)	Use strong US economy vs. Soviet sluggishness to undermine confidence. Aid Afghan fighters to exacerbate quagmire.	Sanctions on exports such as grain & technology. Assistance to states in Africa, Asia, & Europe to deny Soviet access. Rewards to liberalizing satellites.	Encourage Soviet over investment in defense; create economic tensions. Influence behaviors through punishments & rewards.
Technology (export limitations, advanced R&D, investments)	Demonstrate US technical superiority. Undermine Soviet confidence.	Export limitations on useful technologies. Scientific exchanges to reward positive behaviors.	SDI research to regain deterrence & create new calculus, shift Soviet investments, & incentivize bargaining.
Information (exchanges, press releases, speeches, visits, influence in forums, trust building)	Use ideas to influence allies & others to support the US & weaken Soviet influence. Exacerbate tensions in Soviet system; undermine confidence. Counter Soviet propaganda, intelligence gathering, and covert influence.	Influence allies & others to deny Soviets critical resources. Expose Soviet misdeeds. Exploit tensions in Soviet, Warsaw Pact, & satellite governments & populations. Use media campaigns & forums to reinforce evil empire image.	Build relationships with Soviet leaders. Demonstrate superiority of US military, economy, & ideas to undermine Soviet self-confidence. Spread free market ideology to counter Soviet model.
Geography (open ports, proximity, & relationships)	Complicate Soviet strategy, surround & deny opportunities.	Hem in Soviets. Deny access to critical resources. Challenge uses of power.	Complicate Soviet cost-benefit analysis. Raise questions on the utility of their power considering their geographical situation.

Soviet Grand Strategy in the 1980s

An Overview

As with the United States, there are different schools of thought on the Soviet Union's grand strategy in the 1980s. According to Vladislav Zubok, as Brezhnev declined in health after his 1975 stroke, Andropov, Gromyko, and Ustinov became the state's caretakers, leading to a period of stagnation that emphasized military expenditures and undirected global expansion (Zubok 2010: 90-91). From Zubok's perspective, therefore, at least until 1985, the Soviet Union did not have a grand strategy, but reacted to domestic and international developments.

Other scholars posit, however, that the Soviet Union followed a consistent and purposeful strategy based on enduring principles and goals. For instance, several argue that the Soviet grand strategy, which remained largely unchanged since Lenin, was founded on an ideology of expansionism and peaceful coexistence while awaiting the inevitable socialist victory over capitalism (Kintner 1987; Cline 1987). While William Schneider agrees that the Soviets followed a consistent strategy, he posits that it combined opportunistic Bolshevik expansionism with Russian security concerns, was based primarily on military power, and treated allies as subjects rather than coequals (Schneider 1987: 11-12). Similarly, Edward Luttwak argues that the Soviets consistently pursued global superiority, although the goals changed due to their faltering economy and developments in the United States. Thus, although the USSR initially sought to be the leading global economy, it shifted to emphasizing military power, particularly when the US appeared to be in decline (25-31).

Finally, David Gibbs argues that Soviet actions were largely cautious and defensive responses to international events. Thus, from Gibbs' perspective, the Soviet invasion of

Afghanistan was designed to prevent hostile regimes from gaining a foothold on the USSR's periphery rather than an attempt to gain access to a warm water port or increase its influence in southwest Asia. At the same time, while Gibbs acknowledges Soviet military, economic, and information campaigns in Latin America, East Asia, and Africa, he argues that these activities were no more aggressive than US and Chinese foreign policies (Gibbs 1987). Thus, although the Soviet Union did attempt to spread its influence, those efforts were reflective of normal great power competition as opposed to evidence that the USSR was inherently expansionistic.

Although there is a wide range of thought on the Soviet Union's grand strategy in the 1980s, an examination of primary and secondary sources demonstrates that their foreign policy was driven by a set of enduring goals, the approach to which evolved over time due to international and domestic developments. To understand these goals and how the Soviets attempted to accomplish them, in the next sections I will analyze their grand strategic ends and the changing ways the foreign policy executive employed the USSR's elements of national power throughout the decade.

Ends

Any analysis of Soviet intentions during the Cold War inherently faces hurdles due to the limited amount of primary source material available. While a large volume of documents on decision-making in the US during this time has been declassified and digitized, such is not the case with Soviet records. Moreover, even where documents have been released, the process is selective and unorganized, the material is often untranslated, and much of it remains in Russian holdings that are subject to the vagaries of funding and international political forces. Thus, absent resources to access the physical archives and the skills to locate and translate the material, the number of primary sources available is severely constrained.

To mitigate these challenges, I conducted an extensive search for online databases containing Soviet records. Where the records were in English, I used catalogues or key words to identify relevant material. In the case of databases in Russian, I used the DeepL.com tool to translate subject lines and pertinent document texts, which I summarized in an annotated bibliography. I then combined these materials with associated Soviet public statements overt actions, and secondary sources to provide the evidentiary foundation for my analysis.

Through this process, I found that, although the government suffered from internal divisions and thus was not a unitary actor, during the 1980s the Soviet Union nonetheless followed a purposeful, evolving grand strategy that contained four primary ends. First, the Soviets attempted to deter Western attacks on their homeland and interests. This goal, which was arguably their most important concern throughout the decade, was founded on an unshaken belief in the inevitability of socialist victory and a deep distrust of the US and other Western powers (Gorbachev 1986; Brezhnev 1981).

Second, the Soviets sought substantial reductions in nuclear weapons (Gorbachev 1988; Brezhnev 1979). While this goal was initially focused on deterrence and ostensibly upholding the Leninist mantra to seek "peace, prosperity, and international development," as the decade wore on it became increasingly important as a means for reprioritizing resources to address domestic economic challenges (Gorbachev 1988; Chernayaev 1986a; Gromyko 1981: 132-133).

Third, a central element of the Soviet grand strategy was to support socialism's expansion and ultimately win the global struggle for "national liberation, independence, and self-determination" (Gorbachev 1985b; Gromyko 1983: 387; USSR 1977: Article 28). Although a critical and enduring element of the Soviet's foreign policy, this goal inevitably dropped in importance as the FPE recognized their country's dire economic situation and attempted to husband resources to address it (Chernayaev 1986b).

Finally, the Soviets sought to shape US policies, undermine their influence, and divide NATO (Boghardt 2009; Yakovlev 1985; KGB 1985). As with the previous end, this was a long-standing goal that supported the Soviets' efforts to create a favorable international environment for socialism's inevitable victory. In addition, this objective helped the Soviet Union by weakening its adversaries and distracting their resources from offensive efforts. Although this goal became a lower priority as Soviet leaders attempted to deal with growing domestic and economic challenges, it was never abandoned.

Collectively, this analysis demonstrates that, contrary to Zubok and Gibbs, the Soviets were neither predominantly opportunistic nor exclusively defensive-minded. Rather, Soviet foreign policy in the 1980s was guided by a grand strategy that had both offensive and defensive components that evolved in priority over time in response to internal and external forces. In the next section, I will explore the ways the Soviets attempted to achieve these goals.

Ways

While the US enjoyed an expanding set of means during the 1980s, for the Soviet Union the situation grew starker with the passage of time. As the decade wore on, therefore, the FPE became increasingly concerned about the changing international and domestic environments and the seemingly limited means for pursuing their desired ends. This not only shaped their priorities but also forced an evolution in how the leaders applied Soviet elements of national power to achieve their goals.

Deterrence

For the Soviet Union, the military element of power was a critically important tool for achieving deterrence and providing time for the natural process of socialist development to gain success (Brezhnev 1982; Andropov 1982; Chernenko 1984: 390; Gorbachev 1985b: 388). As demonstrated by their operations, deployments, and spending, the Soviets placed heavy emphasis on maintaining a strong, active conventional and nuclear defense to provide a credible deterrent against threats to their homeland or other interests.

This is aptly reflected in their spending patterns, which prioritized defense programs and associated innovation over investments in other areas of the economy, such as non-defense manufacturing (Allen 2001: 867-868). As a result, despite their claims to the contrary, during the first half of the 1980s the Soviet military continued to grow, and the Warsaw Pact maintained numerical superiority throughout the decade (Brezhnev 1979; NATO 1987a).

However, as the economic crisis worsened, the FPE attempted to shift budgetary priorities, reduce tensions with the US, and change their force planning and doctrine to increase technical and professional quality rather than maintaining quantitative parity (CIA 1989; Chernayaev 1988a; Central Committee, Communist Party of the Soviet Union, hereinafter CC CPSU 1986b; Yakovlev 1985). Thus, military reform served to obtain cost savings while simultaneously upgrading defense capabilities to offset the perceived continued threat from the West. Unfortunately for the Soviets, this effort was unsuccessful. Although defense spending did decrease in real dollars, in relation to the GNP it stagnated or even grew, reaching from 9 to 21%

by 1990, depending on what is included in the calculations (Steinberg 1992; International Monetary Fund 1990: 7-8).

From an information standpoint, the Soviets used speeches and articles published in the official newspaper, *TASS*, to communicate their resolve and warn the US and its partners against actions the FPE perceived to be threatening. Moreover, the Soviets engaged in extensive espionage campaigns in the United States, Western Europe and Japan involving the theft of data and designs from scientific research, manufacturing, and by hacking into the nascent computer networks. (CIA 1985b: 19-20). Collectively, these operations likely saved the Soviets billions of dollars in research and development costs and greatly expedited the process of fielding new weapons and technology (20). Moreover, the Soviets maintained an active spy recruitment and handling effort through which they obtained highly sensitive information that allowed them to gain insights on and counter US military operations, communications, and espionage programs (Nye 2015).

Finally, the Soviets used their massive land forces, proximity to Western Europe, and favorable geographic features to credibly threaten NATO countries with a conventional invasion. This threat was exacerbated by NATO's heavy reliance on the United States for support, which involved extended logistical lines that were vulnerable to attack by Soviet naval and air forces (NATO 1987b). Thus, the Soviets took advantage of their interior lines and proximity, which they used to great effect.

Reduce nuclear stockpiles

As with the United States, a consistent Soviet end was to achieve reductions in nuclear weapons. The rationale for this goal, however, came from three disparate sources. First, the

Soviet leadership was earnestly concerned about the risks of nuclear war, particularly after tensions grew nearly to the point of armed conflict early in the decade. Second, highly publicized Soviet offers to negotiate and apparent desires to eliminate nuclear weapons burnished their image as peacemakers (Brezhnev 1982: 515-516; Chernenko 1984; Gorbachev 1985a). Finally, as the 1980s wore on and their economic situation became increasingly dire, the Soviets saw the negotiations as an urgently needed opportunity to reduce military costs (Chernyaev 1986; CC CPSU 1986a; Fakiolas 1998: 82-83).

In the process, the Soviets often used publicity in an attempt to pressure the US into agreements that would allow the USSR to achieve a decrease in nuclear weapons while simultaneously enhancing their relative military power and legitimacy (MccGwire 1991: 60). As one element of this approach, Soviet leaders portrayed themselves as attempting to create a less dangerous world and the West as an intransigent malign actor bent on gaining nuclear superiority (Yakovlev 1985; CC CPSU 1986a; CC CPSU 1986b). This approach played out repeatedly, from an initial stand-off over intermediate nuclear missiles in Europe to negotiations between Gorbachev and Reagan later in the decade.

Moreover, to allow the Soviets to reduce their nuclear arsenal and associated costs while maintaining a credible defense, the Soviets also implemented technological and organizational programs to modernize their military (Chernayaev 1986a; CC CPSU 1986a). These investments were supported by Soviet research and development as well as extensive espionage programs through which they sought information about US intentions, nuclear capabilities, the Strategic Defense Initiative, and related systems.

Support the Global Struggle

For the Soviet Union, which perceived itself as the leader of the global socialist movement, this goal was of central importance to their identity, as reflected in Article 28 of their constitution (USSR 1977). To achieve this end, the Soviets used information, economic, technical and military resources to overtly and covertly support socialist governments and enable proxies that would help them meet their strategic objectives. In addition, the Soviets sought to maintain a strong military to demonstrate socialism's superiority and encourage others in the movement (Gromyko 1981).

One indicator of Soviet priorities in their support for socialist movements was the level of their arms exports, which were provided primarily to achieve strategic and political goals rather than as an income source (Anthony 1998: 71). In the process, from 1980 to 1989, the priority regions for Soviet weapons exports were South and Southwest Asia (45%), followed by Eastern Europe (26%). Africa received 16%, East Asia 7%, and Latin America only 4% (Stockholm International Peace Research Institute 2019). Thus, for the USSR, countries such as India, Iraq, and Iran were of highest importance from at least a military perspective.

In addition to arms exports, the Soviets provided allies, such as Cuba and Vietnam, with support through discount rate oil or by purchasing their commodities at an inflated market price (Anderson 1983). Moreover, the USSR continued their long-standing efforts to contest US influence in developing countries by providing technological and educational assistance (Kochetkova, et. al. 2017). This was particularly true of Latin America, in which the Soviets demonstrated increased interest in the early 1980s as it provided them with an opportunity to expand their trade, enhance their influence in the Western Hemisphere, and support burgeoning global socialist movements (Berrios 1988: 2-4; CIA 1982).

From a defensive perspective, the Soviet Union also worked against perceived US support for counterrevolutions in multiple socialist-led countries, including Afghanistan, Poland, Ukraine, and the Baltics (Gorbachev 1985a; Gromyko 1983; Andropov 1982). This included the extensive use of military advisors, training, and economic assistance, which the Soviets emphasized, was provided at the recipients' requests (Andropov 1981). As an example, in 1983 the CIA estimated that the Soviet Union deployed 19,000 advisors to less developed countries, which sent 4200 trainees to the USSR in return (CIA 1983: 1). These investments were buttressed by information campaigns designed to reinforce the legitimacy of the Soviet Union's actions and to paint Western powers as colonialist interlopers who were undercutting states' sovereignty and the people's right to self-determination (Gromyko 1983: 579-581; Gorbachev 1985a: 196-199; Gorbachev 1986: 706-711).

As with other aspects of the Soviet's grand strategy, however, efforts to achieve this goal changed after 1985 due to political and economic considerations. Specifically, Soviet economic reforms shifted resources to domestic concerns and negotiations with the US led the Soviets to pursue less aggressive methods (Zubok 2010: 105-107; Singleton 1987; Shatalov 1990). Thus, the Soviets did not abandon support for the global socialist movement. Rather, they changed their approach to mitigate tensions with the United States, prioritize key areas of influence, and achieve cost savings (DOD 1989: 19-27).

Shape US Policies and Divide the West

While the military played a critical role in Soviet deterrence efforts, it also was a significant asset in the USSR's attempts to shape US policies writ large. Operations such as their long-range air patrol program, nuclear missile submarine and surface ship deployments, and intelligence gathering ships stationed in Cuba and along the coast of NATO countries not only ensured Soviet military capabilities were well positioned in case of armed conflict but also provided a messaging tool for influencing US and allied behavior (DOD 1985: 7).

In addition, the Soviets also attempted to divide the West through operations to influence US and European internal politics. To achieve this, the Soviets exploited Western peace movements, religious groups, labor unions, and political parties, which they infiltrated and used to create domestic pressure (Kingsbury 2009; US Department of State 1987: 79-85). The Soviets also routinely produced official-looking forged documents that appeared to show US complicity in the AIDS epidemic, racial divisions, and the murders of innocent people (KGB 1985; Schoen & Lamb 2012: 24; Boghardt 2009). To rapidly disseminate the forgeries, the KGB would use Western agents to feed the documents to susceptible newspapers in the form of unsigned letters (Boghardt 2009: 3). In the process, the Soviets relied upon a network of spies to gather intelligence on targetable social problems, relationships, and tension points within and among Western states (Ministry for State Security 1983).

Moreover, the Soviets attempted to portray themselves as peace-seeking and non-aggressive in relation to the West's attempts to impose its values on the world (Chernayaev 1986b). This message was reflected in their public statements and TASS articles in which they urged respect for self-determination while describing NATO countries as malign colonial powers beholden to the arms industry (Gromyko 1983: 583; CC CPSU 1986a; Gorbachev 1986: 707-708). Although Soviet leaders earnestly sought nuclear arms reductions, they also used the negotiations as a platform for communicating their message as peacemakers and exerting public pressure on the US (Gromyko 1981: 132-134; CC CPSU 1986a).

Analysis of Soviet Grand Strategy

The above demonstrates that, although the Soviet Union's grand strategy evolved with internal and external influences, its basic principles endured throughout the decade. To provide the foundation for my model of conflict in the 1980s, in this section I will use the above analysis, applied through the neoclassical realist vulnerabilities, as a framework for evaluating how the Soviets employed their elements of national power to undermine and influence the US grand strategy. The results are reflected in Table 3, below.

International Conflict in the 1980s

As outlined in Chapter One, the purpose of the above historical analysis was to gain a holistic understanding of the United States' and Soviet Union's grand strategies in the latter phase of the Cold War. In this section, I will use the results of that analysis to develop a conceptual model of international conflict during that time frame. To accomplish this, I will discuss the character of conflict in the 1980s as reflected in the states' overarching goals and provide a synthesis of how they employed their elements of national power to achieve their ends. Based on this analysis, I will then create models that capture these conclusions in visual form.

Table 3: Soviet Approach to International Conflict

Variables ElementS	FPE Perceptions	Ability to access & employ resources	Strategic Culture
Military (nuclear & conventional forces, security assistance)	Build & sustain massive military. Train & equip proxies to expand Soviet influence & reach. Operate & deploy forces in proximity to US & allies to showcase capabilities & demonstrate opponent weaknesses.	Use proxy forces to undermine US access to markets, political influence, cooperation, & basing. Military cooperation in Middle East. Large, capable navy, aggressively deployed. Exploit Vietnam syndrome.	Build & demonstrate biggest, fastest, strongest weapons, platforms, & forces. Greater quantity to offset US technology-centric culture. Threat of heavy casualties through nuclear & conventional superiority.
Economic (aid, trade, export controls, sanctions, rewards)	Aid to socialist countries & movements. Heavy investment in defense. Publish deceptive data on Soviet economy.	Favorable relationships with socialist & non-aligned countries to block US access / influence.	Relationships & claims of superior economic performance to undermine US capitalist ideals.
Technology (advanced R&D, investments)	Heavy investment in security related R&D. Showcase in parades, articles, speeches, etc.	Espionage to offset US technology advantages, rapidly advance own capabilities.	Quantity over quality. Espionage to gain advances cheaply & create countermeasures to US reliance on tech.
Information (exchanges, press releases, speeches, visits, influence in forums, trust building)	Deception to confuse & mislead decision-makers. Public speeches & articles in controlled press to communicate positions, enhance image, & demonstrate resolve. Propaganda to show Soviet strength & socialism's superiority.	Forgeries to undermine US / NATO credibility. Infiltrate domestic organizations & movements. Espionage to undermine US / NATO operations security & confidence. Paint West as exploitive vs. Soviet support for self-determination.	Propaganda to demonstrate duplicity in US values-centric arguments, capitalist norms, & support for human rights.
Geography (open ports, proximity, & relationships)	Military bases, insurgencies, & movements in key areas to undermine sense of security.	Exploit position in Europe (favorable attack avenues & internal lines) as well as Asiatic connections & locations.	Use Cuba & other locations in Western Hemisphere to exert pressure on US historical sphere of influence.

Synthesis of Ways, Means, & Ends

The 1980s represented a continuation of the overarching ideological struggle that was central to the Cold War. On a global scale, this manifested in a competition for power and influence in which the states relied heavily upon their military, economic, information, technical, and geographical elements to gain adherents, protect their own spheres of influence, block opponent's expansion, and shape the adversary's behaviors.

Within these elements of power, the military played a predominant role as a mechanism through which to deter unacceptable behaviors, shape policies, and undermine their opponent's sense of security. The US and USSR also used military power to validate their own ideologies, help their foe's adversaries, and create technological, economic, and geographical dilemmas. To achieve these goals, the states deployed conventional and military forces to sensitive regions, invested heavily in security-related technology, and showcased their capabilities through deployments and exercises. They also used their military resources as bargaining tools or to reinforce their negotiating positions, particularly those relating to nuclear weapons.

Information power was also a key element through which the states sought to create or exacerbate domestic divisions, mislead their opponents, undermine alliances, and influence non-aligned governments. Moreover, the US and USSR attempted to exploit and reinforce a good versus evil dichotomy in which the other appeared to be aggressive, self-interested, and destructive to the prospects for peace. In the process, the states used the press, radio, and television broadcasts, as well as speeches in international and domestic forums as dissemination platforms. In addition, the US and USSR routinely used espionage, conducted by moles or recruited spies, to understand the other's intentions, offset military, technological, or economic advantages, and to inform their own operations. These activities had the additional benefit of creating uncertainty and suspicions, with their attending internal tensions and the diversion of resources to counterintelligence and security operations.

Economically, the US and USSR used their power to invest in military build-ups, support and influence existing and potential allies, and provide rewards or inflict punishments on other states. Due to the largely closed Soviet system, their degrading economic situation, and limited trade between their bloc and Western allies, however, economic power increasingly favored the West as the decade wore on. As a result, this asymmetry slowly changed the character of the conflict as the Soviets were forced to shift their resources away from investments in the military, technology, and the socialist system in an attempt to shore up their flagging economy.

Technologically, both powers sought to use scientific advancements to gain military and economic superiority. As with economic power, the US and USSR would share technology with others as a reward or withhold it where the state engaged in unacceptable behavior. Espionage also played a fundamental role in this realm, particularly for the Soviets who employed networks of well-placed scientists, employees, and officials to steal information on technological advancements both to offset any US advantages and to provide a leap forward in technology without the requisite investment of money, manpower, and time.

The US and USSR employed their geographical power in three main ways. First, both states contained vast resources and territory, which they used to support their other elements of power. Second, the states used allies, bases, and favorable geographic features to negatively affect the adversary’s sense of security and spheres of influence. While these efforts were global in nature, they were highly concentrated in Europe and Central America. Finally, the US and Soviet Union threatened the other’s sea and land lines of communication (LOCs) by placing or operating military assets at choke points, along open coastlines, or in other locations where they could interdict efforts to access and deploy resources. They also used the open sea lanes and air routes to fly long range bombers and reconnaissance aircraft or to sail missile and sensor carrying ships and submarines. These assets provided the opposing state with close-in surveillance and deterrence capabilities that, but for the attending geographical features, would not have been possible. The above can be summarized as reflected in Table 4, below.

Table 4: International Conflict in the 1980s

Variables Elements	FPE Perceptions	Ability to access & employ resources	Strategic Culture
Military (nuclear & conventional forces, security assistance)	Deter behaviors, shape policies, & undermine opponent's sense of security. Challenge other's ideology. Showcase or hide capabilities to shape perceptions of power.	Build & sustain proxy forces to undermine opponent's access to markets, political influence, cooperation, & basing. Create dilemmas for other elements of power.	Impact cost-benefit analysis. Use military power to shape other variables & elements. Exploit cultural fears (Vietnam / foreign invasion).
Economic (aid, trade, export controls, sanctions, rewards)	Aid to allies & proxies to build network & offset opponent expansion. Strengthen defense.	Favorable relationships with other states & proxies to block opponent's access & influence.	Display strong economy to support own ideology, undercut opponent's.
Technology (advanced R&D, investments)	Use scientific advancements to gain military & economic superiority. Showcase in parades, articles, speeches, etc.	Espionage to expand capabilities & offset strengths. Rewards & punishments to deny opponent's influence / access to other states.	Use quality or quantity to offset the other's preferred approach.
Information (exchanges, press releases, speeches, visits, influence in forums, trust building)	Mislead opponent, undermine alliances, & influence non-aligned states. Speeches, radio, TV broadcasts, & articles to communicate positions, enhance image. Demonstrate resolve.	Exacerbate domestic divisions, undermine credibility. Espionage to undercut security & confidence. Manipulate good vs. evil image. Paint opponent as inherently destructive to people's well-being.	Influence campaigns to demonstrate duplicity in other's arguments & actions. Raise questions about other's values, capabilities, & assumptions.
Geography (open ports, proximity, & relationships)	Support other elements of power. Use allies, bases, & favorable geographic features to negatively affect the adversary's sense of security.	Threaten other's LOCs. Exploit open coastlines, & other locations to deploy interdiction forces & surveillance capabilities. Shape opponent's ability to use resources.	Undercut opponent's historical spheres of influence, especially in Europe & Latin America.

Conflict Models

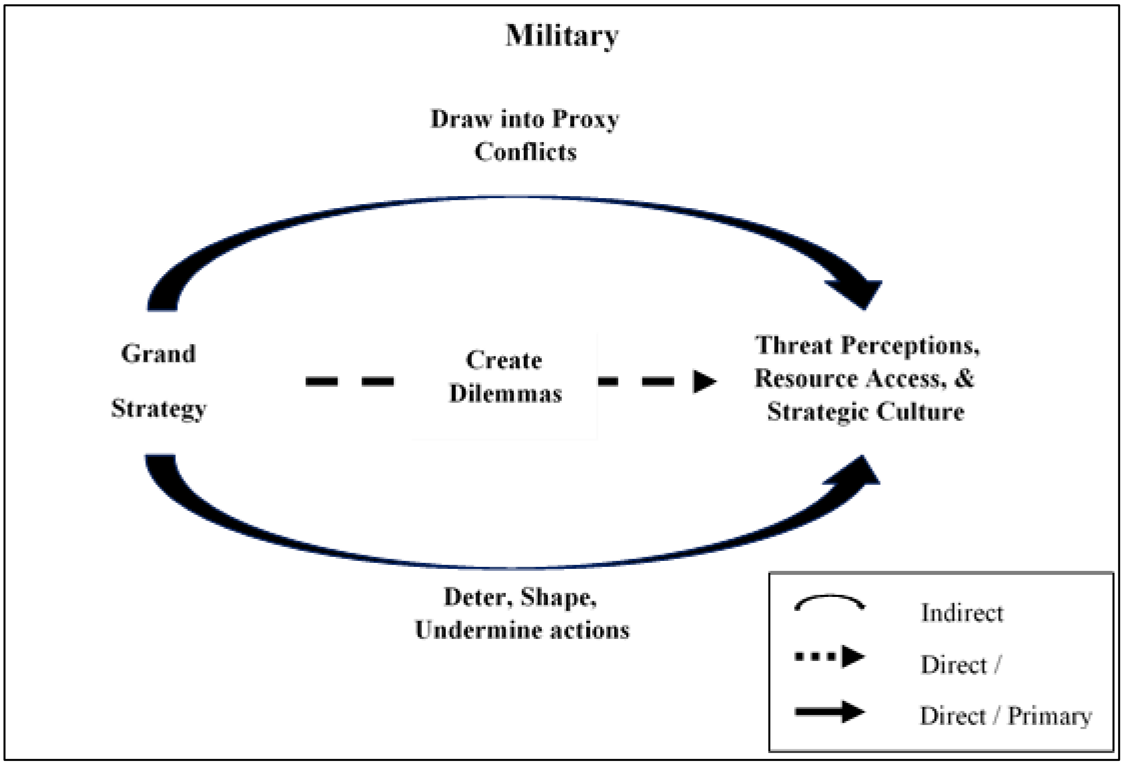
While the above matrix provides a useful framework for understanding how the states collectively employed their elements of power, to provide a foundation for comparison with the New Era of Conflict it is necessary to analyze the conclusions through the lens of my research theory. Specifically, to evaluate whether the revolution in cyber technology is changing international conflict by enabling actors to directly impact states' grand strategy formation, we must understand the 1980s in terms of the ability of the great powers to use their elements to directly or indirectly influence their opponents' neoclassical intervening variables.[3]

To facilitate this process, I have developed visual models that demonstrate how the states directly or indirectly employed their elements of power (Diagrams 3 through 7). As these schematics demonstrate, in the 1980s the military was primarily used to create indirect effects against the opposing power. This was largely a result of the states' desires to avoid armed conflict and to reduce conventional and military arms. The other elements, however, played both direct and indirect roles, as the US and USSR built alliances, shaped other states' behaviors, and created immediate effects on the opponent's economies, decision-making, and resulting policies.

It is important to note, however, the critical role information played in the conflict. As reflected in the diagrams, the element predominated as the states used it for multiple direct and indirect purposes. Although the military received the highest level of financial investment, information nonetheless proved invaluable due to the ideological nature of the conflict and its

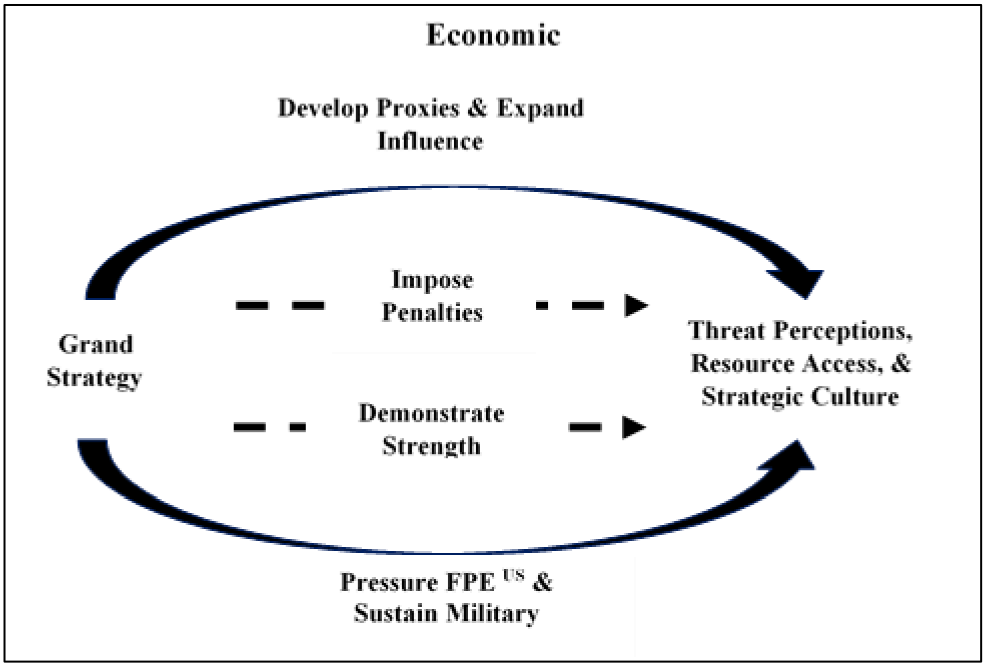
[3] Direct includes the use of an element to produce an immediate effect without an intervening party or other influence. Indirect, however, is the use by or through a third party or in a way that does not employ the capability to its full, traditional extent. For example, direct use of the military would be a kinetic strike, while indirect use would be using it to deter an opponent.

utility in shaping behaviors and supporting other elements with limited risk of escalation. Moreover, due the United States' more favorable financial conditions, it relied more heavily on the economic element of power to directly impact the Soviet Union. Thus, while there were a lot of similarities in how the states approached the conflict, one area where they diverged was in their employment of economic power.


Military
Draw into Proxy Conflicts
Grand Strategy
Create Dilemmas
Threat Perceptions, Resource Access, & Strategic Culture
Deter, Shape, Undermine actions
Indirect
Direct /
Direct / Primary

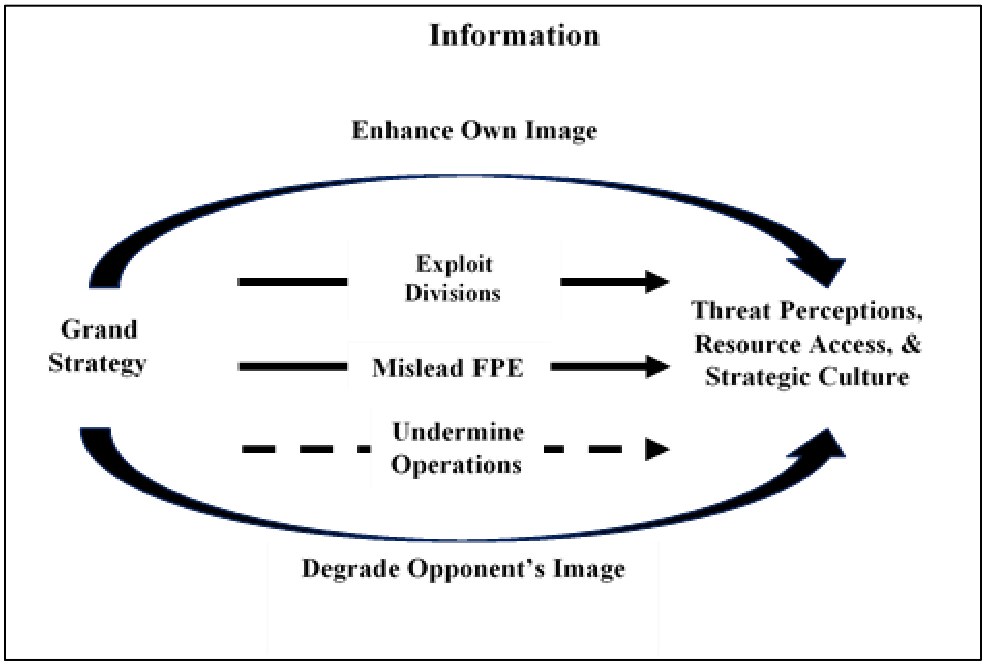
1980s Military Conflict Model

Diagram 3



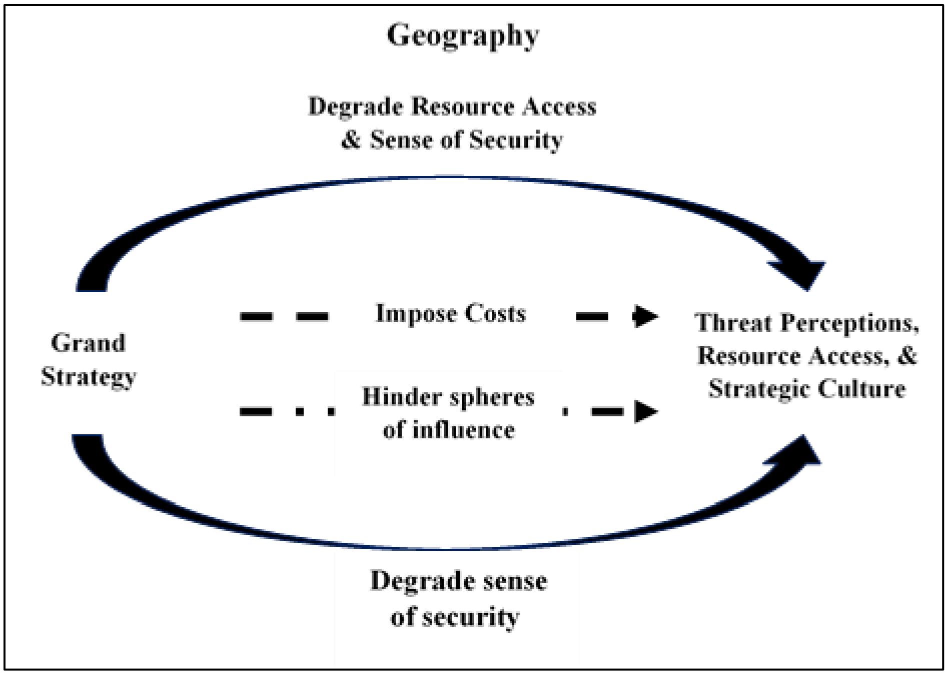
1980s Economic Conflict Model

Diagram 4



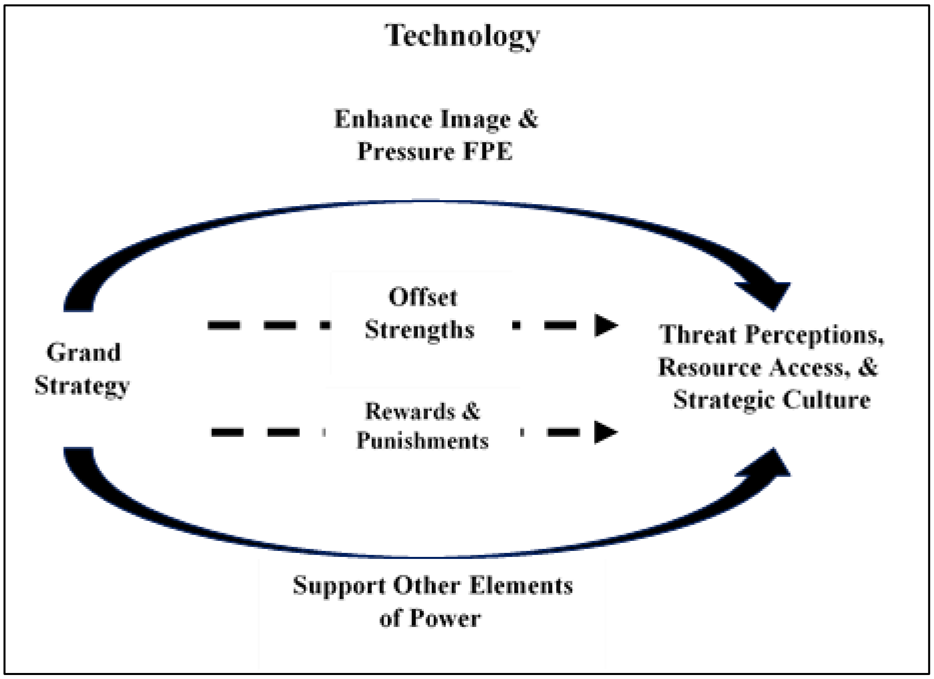
1980s Information Conflict Model

Diagram 5


Geography
Degrade Resource Access & Sense of Security
Impose Costs
Grand Strategy
Hinder spheres of influence
Threat Perceptions, Resource Access, & Strategic Culture
Degrade sense of security

1980s Geographic Conflict Model

Diagram 6


Technology
Enhance Image & Pressure FPE
Offset Strengths
Grand Strategy
Rewards & Punishments
Threat Perceptions, Resource Access, & Strategic Culture
Support Other Elements of Power

1980s Technology Conflict Model

Diagram 7

Thus, although the Cold War is often characterized as a competition for relative material power in the international arena, it was more complex and nuanced than these arguments suppose. Rather, while the military and economic elements played critical roles in how the conflict evolved and ended, information was central to the grand strategies that each state employed. As I analyze the New Era of Conflict in the next chapter, and ultimately compare the two periods, this is an important consideration in how power was defined and used, and how international conflict was characterized during the 1980s.

Conclusion

The purpose of this chapter was to provide a pre-cyber era case study as a comparative baseline for the New Era of Conflict. To accomplish this, I conducted a detailed examination of the US and USSR's grand strategies during the 1980s from the standpoint of their elements of national power. I then analyzed how the states employed those elements to undermine their opponent's neoclassical intervening variables and synthesized the results. Finally, I used the outcomes to develop a holistic conceptualization of great power conflict during the decade.

Collectively, this analysis demonstrated that, while international conflict in the 1980s involved all elements of power, the states relied most heavily on military and information capabilities, which provided them with avenues for indirect and direct approaches, respectively. While the other elements of national power, geography, economy, and technology, each contributed to the conflict, they were typically secondary, supporting efforts.

These conclusions are important for two reasons. First, although the Cold War is often characterized as a competition for superiority in relative material power, the above analysis indicates that information played the leading role. This is evident in the finding that, while the states were obsessed with economic performance and spent exorbitant amounts of money on building, sustaining, and operating their forces, the resulting capabilities were rarely used to engage in direct conflict with their main opponent. Instead, the economic tool supported the US and USSR militaries and was used to pressure the other state, while the military served as a symbol of ideological superiority, a counter to expansion, and a preventative measure against a global conflagration both sides knew they would lose. In the process, the economic systems largely remained isolated from each other while the military was deployed around the world, or used in proxy battles, to deter and shape the other state's actions.

At the same time, however, the US and USSR understood that, as long as the other's ideology maintained sufficient influence with key populations and leaders, and the other elements were not dramatically weakened, the conflict would continue. As a result, the respective FPEs relied heavily upon propaganda, speeches, press releases, and other manifestations of information power to directly undermine the other's ideological foundations, shape their perceptions, create divisions within their domestic populations and international alliances, and attack the foundations of their strategic cultures.

Second, these conclusions raise questions about how power was defined in the 1980s. While the basic realist assumption is that power was largely a measure of relative material factors, the above indicates that it contained multiple components and served as a means for furthering national objectives rather than "an end unto itself" (Ripsman, et. al. 2016: 44; Mearsheimer 2001; Waltz 1979). Thus, power in the 1980s was more nuanced than is often appreciated, particularly by the structural realist school of thought.

At the same time, however, it is important not to overstate or overinterpret the above results. Rather, for the US and USSR, military and economic power were important components of how they saw themselves and their adversary. For the great powers, and other states within the system, the numbers of ships, aircraft, missiles, and soldiers, and the relative growth of their gross national products, were key metrics in how the conflict was progressing. Thus, Waltz and other structural realists were partially correct in that power had a distinctly material aspect, although the states' conduct demonstrates that other elements, particularly information, were fundamental to the character and conduct of the conflict.

The key questions that remain are whether international conflict and the definition of power have changed and, if so, what role cyber technology played in the process. To provide the foundation for this analysis, in the next chapter I will examine the US and Russian grand strategies in the New Era of Conflict (2007-2018) using the same methodology as above. This will provide a solid comparative case for understanding how the states are engaging in international conflict in the cyber era. In the final chapter, I will identify differences between the two time periods and examine the role cyber technology played in the changes. As a part of this, I will also examine whether the meaning of power has changed and, if so, how. Taken together, this analysis will demonstrate what changes have occurred and why.

Chapter Five: The New Era of Conflict (2007-2018)

Introduction

In April 2007, the Estonian government decided to move a Cold War era statue of a Soviet soldier to a less prominent location in its capital, Tallinn. In response large segments of the ethnic Russian population rioted and Estonia suffered three weeks of increasingly complex cyberattacks on its commercial and government infrastructures (Tikk, Kaska, & Vihul 2010: 23-24). As an early adopter of cyber technology, the state was particularly vulnerable to such attacks, which disrupted civil services, external communications, and the banking industry. Although the Russian government denied involvement, the sophisticated nature of the attacks and location of some IP addresses indicate that it at least played a supporting role (Saltzman 2013, 52; Blank 2008b).

This event, which marked the beginning of increased Russian assertiveness on the international stage, was the opening salvo in the New Era of Conflict. While Russia had become more bellicose in prior years, 2007 represented a sea change in the scope and amplitude of its behavior. A year after the Estonia attacks and riots, Russia invaded Georgia, ostensibly to protect the Russian population in the breakaway province of South Ossetia, but more likely as a countermeasure to Georgia's growing relationship with the West (Cohen & Hamilton 2011: 1-3). This was closely followed by Russia's increased efforts to use frozen conflicts in Moldova, Azerbaijan, and other states in its near abroad to provide a buffer, establish its military outside its borders, and pressure victim governments into adopting more favorable policies (Grossman

2018: 52-53; Veebel & Ploom 2016: 54). Then in 2014, Russia engaged in the first post-Cold War seizure of another state's territory when it invaded and then annexed Crimea. This, combined with its sponsorship of a separatist uprising in the Donbas region of Ukraine as well as persistent cyberattacks against the country's critical infrastructure, represented a purposeful attempt to force Kiev to move away from the West after Ukrainian protests overthrew its Moscow-friendly government.

The assertiveness, however, was not limited to invasions or proxy conflicts in Europe, as Russia also assassinated perceived adversaries in England and Germany, launched extensive propaganda campaigns against Baltic governments, intervened militarily to save Syria's much maligned leadership, and increased long range aviation, surveillance ship, and ballistic nuclear submarine patrols in close proximity to NATO partners. In addition, President Vladimir Putin developed an ever-closer relationship with China, Turkey, and Egypt, attempted to influence election outcomes in the US and France, worked to create parallel monetary and security systems, and supported the Venezuelan regime in its struggle against US and European efforts to force its autocratic president to leave office (Kremlin 2019h).

For the US and many Western observers, particularly those in Russia's near abroad, these behaviors represented extreme and unacceptable attempts to change the post-World War II liberal order and to recreate the Soviet sphere of influence (Rumer & Sokolsky 2019). Putin, however, argued that they were necessary countermeasures to US unilateralism and its aggressive attempts to isolate Russia and undermine its stability (Radin & Reach 2017: 32-35). Despite periodic attempts to mitigate these inherently incompatible perspectives, however, the relationship between the US and Russia grew increasingly tense, as their behaviors reinforced the other's fears and a chronic state of conflict developed.

In this chapter, I will argue that these developments marked the first phase in a new global conflict between the US and Russia in which cyber technology played a fundamental role. To examine this argument and set the foundation for my comparative analysis with the Cold War in the next chapter, in this case I will focus on four main questions. First, what were Russia and the United States' grand strategic goals in relation to each other? Second, how did they employ their elements of national power to achieve these ends? Third, how did the states exploit cyber technology to support their grand strategies? And, taken together, what do these approaches tell us about great power conflict in the 2007 – 2018 time period?

To accomplish these goals and explore the argument, in the following sections I will analyze each state's grand strategy through the lens of the neoclassical realist framework. In the process, I will first establish the conflict's historical setting by examining the international environment during the 1997 – 2006 and 2007-2018 timeframes. Next, I will dissect each state's grand strategy by analyzing the United States' and Russia's approaches through an ends, ways, and means framework. In addition, to provide the foundation for evaluating my hypothesis, I will specifically call out how cyber technology was used in the conflict. Third, I will examine how each state sought to use its elements of power to exploit the vulnerabilities created by the neoclassical realist intervening variables in their opponent's decision-making process. Finally, I will synthesize these findings and use them to develop models that will visually represent international conflict during the period. Collectively, these steps will provide the baseline for a comparative analysis of the Cold War and the New Era of Conflict in my final chapter.

Historical Setting: 1997-2006

With the end of the Cold War and the collapse of the Soviet system at the beginning of the decade, the 1990s held the promise of enduring peace. Unfortunately, while scholars heralded a victory for international liberalism and predicted the inevitable expansion of democratic principles across the globe, troubling undercurrents soon challenged their utopian dreams. As with the post-World War II era, the realities of the international system once again predominated, as power struggles within and between states did not dissipate but expanded in scope and violence as long repressed grievances and ethnic tensions rose to the surface.

For the United States, these developments presented both promise and peril. Suddenly the sole remaining superpower whose homeland seemed secure from any viable threats, the US had at its disposal tremendous military and economic might as well as legitimacy as the victor of the long-enduring ideological struggle. Despite its overwhelming strength, however, the United States was unable to prevent Yugoslavia's implosion, warlord rule in Somalia, genocide in Rwanda, the rise of al Qaeda, and nuclear proliferation to South Asia. Collectively, these and other events demonstrated the limits of US power and led to soul searching over how to define its interests and role in the new world order.

Caught in the middle of these developments, the Clinton administration implemented a grand strategy that sought to exploit the peace dividend by reducing US military outlays and relying on international institutions to create stability and expand liberal ideas into former Soviet spaces. As a result, from 1992 to 1998, the US cut total military spending by 10%, and reduced foreign deployments by 26% while simultaneously working to expand NATO's footprint and contributions to UN peacekeeping operations (DMDC 1992; DMDC 1998, 12; Masters 2019;

World Bank 2019i). This trend was not long enduring, however, as growing concerns about US national security spurred increases in military spending, which expanded by 7% in 1999 and 2000 (World Bank 2019j). What began as a slow expansion, however, became frenetic after the September 11th terrorist attacks, with military spending increasing by 88% between 1999 and 2006, reaching $527.6 billion (DMDC 1999: 12; DMDC 2005: 11; World Bank 2019j).

Economically, the US also expanded, as the GDP grew by $4.7 trillion with an average increase of 4.4% per year from 1997 to 2000 (World Bank 2019l). Although the US dipped into a short recession in 2001, it rebounded to achieve a collective increase of 2.9% over the next five years (World Bank 2019c). Collectively, from 1997 to 2006, the US economy grew by an additional $5.2 trillion, reflecting a 12.8% increase (World Bank 2019c). Meanwhile, its nearest competitor, Japan, had settled into economic stagnation, and China, which was beginning its rapid growth, had an economy only one fifth its size (World Bank 2019f; World Bank 2019a).

Alternatively, for Russia the military and economic situation held far less promise in the 1990s. After the Soviet Union's collapse, military spending experienced a seesaw over the decade, rising and falling by up to 44% before undergoing sustained growth after Vladimir Putin came to power in 1999 (World Bank 2019h). Similarly, Russia's economic performance was largely negative, dropping from a GDP of $516.8 billion to $195.9 billion between 1990 and 2000 (World Bank 2019j). Russia was also in heavy debt and had limited and dwindling foreign exchange reserves (Gaddy 2007: 38). Yet, due to increased oil and gas revenues, strong domestic consumption, and Putin's imposition of disciplined corruption, by 2006 the Russian debt load had been largely paid off and its GDP had grown to $989.9 (41-43; *The Economist* 2007; World Bank 2019j). Although these were significant improvements, Russia's military still suffered from archaic equipment and low morale, and its economy was still relatively small (Haas 2011: 12-13).

From a geographical perspective, despite the United States' initial struggle to define its post-Cold War role, after the September 11th terrorist attacks it adopted an aggressive foreign policy that saw its military presence increase in key regions, including the Middle East, North Africa, and South Asia. In addition, the US continued to support NATO's expansion, with ten countries joining the organization between 2000 and 2006, all of which were former Soviet states or satellites (NATO 2019a). This expansion, together with the ostensibly US-sponsored color revolutions in Serbia (2000), Georgia (2003), Ukraine (2004), and Kyrgyzstan (2005), created tensions between the two states as Russian leaders increasingly perceived that they were being surrounded and their hold on power threatened by Western interference (Bērziņa 2014).

In addition to pressures from the near abroad, Russia struggled with domestic instability. As the newly installed premier, Putin faced significant problems with organized crime and terrorism. Events such as the Moscow theater attack (2002) and Beslan school siege (2004), in which hundreds were killed, only exacerbated Russia's sense of insecurity. In response to these attacks and the ongoing Chechnyan uprising, the Russian government responded heavy handedly, using armor, gas, bomber aircraft, and other military force to suppress the terrorist threat, often killing hostages in the process (European Court of Human Rights 2017; 2011). At the same time, Putin abandoned his conciliatory outreach to the West and began using increasingly pointed language, accusing the US and NATO of being predatory (Lomagin 2007: 42). While there was significant domestic and international condemnation of his response to the terrorism incidents, Putin's popularity remained high in Russia, as many saw him as a tough defender who was taking the necessary steps to defend the state (*The Economist* 2016).

Technologically, the US was particularly strong during the 1990s and early 2000s. For instance, according to an Organization for Economic Cooperation and Development (OECD) study of the telecommunications industry in 2005, US companies were some of the largest and they represented the majority of firms in three of the six technology sectors (OECD 2006: 49-54). In addition, as the hub for internet development, management, and innovation, the US held substantial sway over its direction and related industries. As for Russia, while it did not appear in any of the large industry comparisons, it nonetheless was listed as one of the top seven emerging information and communications technologies (ICT) economies, with clear growth occurring in all sectors (62). Thus, as with many of elements of power, the US dominated while Russia attempted to recover.

One area where this pattern was not followed, was with the states' soft power, which declined over the decade (McClory 2018: 42). Specifically, while the US initially garnered broad international support after the September 11th attacks, subsequent actions, particularly its counterterrorism operations, invasion and mishandled occupation of Iraq, and mistreatment of detainees, caused significant negative repercussions to its influence and reputation (Wike 2011: 1-2). When combined with domestic problems, such as the contested 2000 elections, growing budget deficit, and the Bush administration's inadequate response to the Hurricane Katrina disaster in 2005, these challenges raised questions about the state's effectiveness, legitimacy, and longevity as a superpower (*The Economist* 2005). Russia too, suffered significant international blow back from its policies, as the Putin administration struggled to address domestic terrorism and perceived threats in its near abroad (Avgerinos 2006: 115-116).

Collectively, this demonstrates that, for the United States and Russia, the decade before the New Era of Conflict was a time of both growth and uncertainty. While the US dominated militarily, economically, geographically, and technologically, it nonetheless suffered significant setbacks to its soft power and faced serious questions over the limits of its material means. As for Russia, despite its incredible recovery from economic, military, and social collapse following the Cold War, significant domestic challenges remained. To make matters worse, Russia faced what seemed to be an increasingly unfriendly international environment. These circumstances, and the perception that US was largely to blame for Russia's ills, set the stage for the next decade and were the impetus for the New Era of Conflict.

The New Era of Conflict: International Stimuli (Means)

In 2007 the world was on the precipice of change. Economically, that year marked the beginning of a global downturn that resulted in the direct loss of an estimated $4 to 19 trillion in US production, ushered in the longest period of unemployment above 8% since the Great Depression, and exacted unknown economic, emotional, and other costs (Atkinson, et. al. 2013: 2; GAO 2013: 12-17). Although the US GDP began expanding again after 2009, annual growth remained below 3% through 2018 (World Bank 2019c).

The impacts were not limited to the US, however, as the crisis reverberated around the world, generating varying losses from minor GDP contractions in Asia to an over 6% reduction the European Union's economy (Verick & Islam 2010: 20-21). As the source of the downturn, many blamed the United States, which, combined with the West's slow recovery, raised fundamental questions about the US-led global economy and drove states to begin looking at alternative economic relationships.

While the world struggled to recover economically, it also experienced dramatic social unrest. Starting in Tunisia in 2010, large scale protests spread across North Africa and the Middle East. Angered by economic inequality and government repression, people called for substantial changes, including fundamental political and economic reforms. Although linked in many of their themes and approaches, the movements had varying effects, including leadership changes in Egypt and Tunisia, increased state repression in Bahrain, and chronic civil war in Libya and Syria. In many places, extremist elements and state proxies exacerbated and exploited the instability, leading to widespread violence. As a result, by 2018 the conflicts had inflicted over 500,000 civilian deaths and generated nearly 15 million displaced persons (Human Rights Watch 2019).

This was particularly true of Iraq, as US attempts to extricate its military created dramatic ripple effects. Despite initial success following the 2007 US military surge, destabilizing factors, such as the central government’s lack of legitimacy and struggles for power among Iranian surrogates, Sunni elements, and the occupying forces, created a violent milieu that spread across much of the country. Exploiting the resulting power vacuum and instability, al Qaida in Iraq rapidly grew in numbers and military strength. Rebranded as the Islamic State in Iraq and Syria (ISIS) in 2013, it built a modern mechanized army that drew in recruits from over 100 other countries.

Startlingly successful, ISIS conquered vast swaths of Iraq and Syria, creating a self-proclaimed state with approximately 41,000 square miles of territory, a population of eight million people, and an estimated monthly revenue of $81 million (IHS Markit 2019; DOD 2017). ISIS also launched a global terror campaign, establishing eight branches in Africa and Asia, and inspiring attacks across the Middle East, Africa, Asia, Western Europe, and North America. Despite the combined efforts of sixty-nine nations, it took over three years to defeat ISIS' conventional army, and the terrorist organization still remains a threat in 2019 (US Department of State 2019a; DOD 2017).

Meanwhile, the United States military continued to engage in combat operations in Afghanistan and other locations, while also maintaining an average presence of 361,000 personnel in 164 countries each year (DMDC 2008 – 2018). This pace imposed a tremendous strain on military members and the financial costs were extensive, with an estimated total expenditure of over $1.56 trillion in "war funds" from 2001 to 2017 (GAO 2017b: 22). These costs, along with a loss of revenue due to the Great Recession and increased non-discretionary expenses, caused the national debt to rapidly increase from $9 trillion in 2007 to over $13.6 trillion in 2010 (Statistica 2019f). In response, Congress imposed spending ceilings, which reduced US defense outlays from $711 billion in 2011 to $596 billion in 2015, before increasing again to $649 billion in 2018 (World Bank 2019i; Harrison 2016). Regardless of the attempted cost controls, however, US debt continued to climb, reaching $21.5 trillion in 2018 (Statistica 2019f).

For Russia, this period was no less challenging, as it faced repeated economic downturns due to the Great Recession, oil price fluctuations, and Western imposed sanctions. While GDP growth had hit a peak of 8.5% in 2007, it dropped precipitously to – 7.8 in 2009, before seesawing from 4.5% (2010), to – 2.3% (2015), then to 2.5% (2018) (World Bank 2019b). At the same time, following its successful but cumbersome invasion of Georgia in 2008, Russia launched an extensive reform of its military, increasing investments from $43.5 billion current US dollars in 2007 to $88.4 billion in 2013, before reducing them to $61.4 billion in 2018 (World Bank 2019i). In the process, Russia transformed its military from an archaic Soviet-era model to an organization that is much smaller, more professional, technologically advanced, and diversified in capabilities (Kofman, 2018: 21). Despite the extensive reforms, however, in 2018 Russia still had significantly less military power relative to the United States, except in the category of nuclear weapons.

Regardless of the security investments, Putin still suffered significant setbacks internationally and was faced with growing political pressures at home. Emblematic of the former were the 2013-2014 Euromaidan protests and subsequent revolution that overthrew Ukraine's Putin – friendly government in favor of one that pursued a closer relationship with the EU (Minakov 2018). Adding to the concerns, throughout the 2010s, large scale protests erupted in Moscow and other cities in response to claims of rigged elections (Kolstø 2016: 704). The resulting sense of insecurity and perception of Western meddling are evident in Russia's policy documents and Putin's speech after his much – maligned 2012 reelection, in which he suggested foreign powers were actively attempting to destroy the state (Luxmoore 2019; *The Guardian* 2012; Ministry of Foreign Affairs 2013).

Exacerbating the economic, social, and military uncertainty for the US and Russia, during this time China became increasingly assertive on the world stage. As its economy continued to grow at a dramatic rate, averaging 8.6% during this period, China invested heavily in defense. As a result, its military spending surpassed Russia's in 2008, continuing to increase thereafter, reaching $250 billion in 2018 (World Bank 2019a). This growth in economic and military power was reflected in China's increased international assertiveness, as it issued a new strategy, adopted an aggressive stance in the South China Seas, and diligently worked to create an Eastphalian international order based on a network of subservient states in Asia, Africa, and Europe (Peng, et. al. 2010; Jacques 2009: 328-329). For the US and Russia, these developments only created more uncertainty, as an assertive China played an increasing role in their foreign policies and raised questions about the future of their power on the international stage.

Due to these and other events, and despite an attempted reset in relations, tensions between the US and Russia only increased over time (Nation 2012: 381-383; Zygar 2016: 173). For Russia, the United States' continued support for NATO expansion and its real and perceived sponsorship of regime change in other countries was deeply disconcerting, as these developments only exacerbated its long-standing fears of being encircled, isolated, and undermined (Kotkin 2016; Lipman 2016). On the US side, Russia's unpredictable behaviors, unresponsiveness to countermeasures, and flagrant violations of long-standing norms, created the sense that it was actively attempting to undermine US power and the international order it leads (Rumer & Sokolsky 2019: 2-3). As a result, and as will be detailed below, the states increasingly found themselves at odds, and in conflict across their elements of power in what many see as a new Cold War.

US Grand Strategy in the New Era of Conflict

An Overview

During this period of study, the United States was led by three administrations with perceptively different foreign policies. From George W. Bush's aggressive foreign engagement, through Barack Obama's apparent retrenchment, to Donald Trump's seemingly chaotic America first approaches, it is arguable that the US followed three disparate grand strategies, or none at all (Martel 2015: 1). At the same time, some scholars argue that the differences among the grand strategies are more apparent than real, as there was significant continuity in the administrations' policies (Dombrowski & Reich 2018: 56-57). Before analyzing the US grand strategy during this period, therefore, it is important to understand whether there was substantial inter case variation that must be accounted for in the subsequent analysis.

For the Bush administration, the post-911 trauma and perceived historical opportunity to rewrite the political map drove an aggressive foreign policy that relied heavily on the United States' coercive capabilities, primarily its military power. In the process, the administration conflated the doctrines of preemption and prevention, adopting an interpretation of international law that allowed it to use force or threats against any state or non-state actor it perceived might present a future threat (Gaddis 2005b). Furthermore, seeking to operationalize democratic peace theory, the US implemented an expansive Wilsonian foreign policy founded on the assumption that democratization, economic liberalization, and cooperation among like-minded states would lay the foundations for international stability and security (Smith 2017; Gaddis 2011; White House 2006). In short, the Bush administration saw the world as a threatening chaos that required the forcible imposition of American values to save it.

When Barack Obama came into office in 2009, the foreign policy he adopted was a specific repudiation of the Bush doctrine. Recognizing the financial and reputational costs of his predecessor's approach, Obama initially sought to maintain US leadership while attempting to husband its resources, rely more heavily on international institutions and foreign partners, and shift emphasis from the Middle East to East Asia (Brands 2016: 101-102; White House 2010). These themes, however, became less pronounced in Obama's second term, due to Russia's actions, particularly in Ukraine and the 2016 elections (White House 2010). Thus, for Obama, the international system presented dwindling opportunities that required the judicious use of US power to protect and exploit them.

Similarly, Donald Trump also claimed that his foreign policy represented a wholesale change from his predecessor, which he saw as surrendering US interests to foreign entities and facilitating the rise of international terrorism (White House 2017: I-II). As a result, where Obama had sought to build conciliatory relationships with foreign powers, Trump argued that the United States needed to disengage from its expensive engagements and renegotiate many elements of the international system, which were unfair to the United States and undermining its power (Sestanovich 2017; White House 2017: 1-4). For the Trump administration, therefore, the international system was dangerous and unfair, and therefore required renegotiation.

While some authors argue that Trump abandoned the United States' leadership role and was actively undermining the post-World War II order, in practice his policies differed from previous administrations largely in emphasis (Daalder & Lindsay 2018). Specifically, Trump's approach differed from Bush's and Obama's mainly in that he focused on enhancing the United States' return on investment. In the process, the Trump administration did not abandon the order's underlying liberal values, but emphasized US interests, which inherently include maintaining the free market, preserving US leadership, and supporting human rights.

Thus, while it initially appears that each administration adopted substantively different grand strategies, their approaches also shared fundamental continuities. Specifically, across the board, successive presidents pursued common goals, including maintaining US global leadership, reducing the threat of terrorism, preventing nuclear proliferation, and protecting the United States' broadly defined interests. In addition, the strategies emphasized similar means, primarily pursuing their goals through coercive power.

This is aptly reflected in how the United States employed its military throughout the period. Specifically, although the total numbers of personnel deployed overseas consistently fell from 2008 to 2018, successive presidencies compensated by greatly expanding the use of drones to strike targets in the Middle East and Horn of Africa (Serle & Purkiss 2017; Bergen & Tiedemann 2011; DMDC 2007-2018). In addition, the US dramatically increased its use of economic sanctions and employed its other elements of power to protect its interests and offset challenges presented by rising states such as Russia and China (Gilsinan 2019).

As such, while scholars and commentators argue about Bush's preemption, Obama's retrenchment, and Trump's chaotic illiberalism, the differences among their policies are more a matter of emphasis and evolutionary development than fundamental divergences in their grand strategic designs (Posen 2018; Dueck 2015; Gaddis 2005b). Where changes were made, they were largely due to domestic political forces, threat prioritization, and the adjustment of tools to address them, as opposed to wholesale deviations in the strategies themselves. How this played out vis á vis Russia, will be analyzed below.

Ends

As reflected above, while the US grand strategy throughout this stage in the New Era of Conflict was based on consistent central tenets, it nonetheless evolved due to international and domestic influences. This is particularly true of the US relationship with Russia, which tended to be cautiously optimistic in the early phases of each administration but became increasingly fraught as strains inevitably reemerged due to chronic disagreements over contentious issues (Light 2008; Gordon 2001). In addition, although tensions were initially focused in Europe, where US and Russian interests most directly collided, the conflict rapidly expanded to other regions and across all physical, virtual, and cognitive domains. In a change from the US – Soviet relationship in the 1980s, therefore, conflict between the two powers did not diminish but increased over time, despite attempts to build better relationships (Burns 2019).

Even while the struggle ebbed and flowed, the US strategy nonetheless remained centered on three primary goals. First, the highest priority was to protect US territory and its interests against Russian interference and attack. Although this end was not a major consideration in the Bush and early Obama presidencies, it grew in importance as the US gradually realized that it was in a conflict with Russia (White House 2006; 2010; 2015). This was particularly true of the Trump administration which, due to existing policies and Russia's continuing assertiveness, and despite the administration's efforts to mitigate the conflict, had little real opportunity to reverse the trend (Haddad & Polyakova 2018; Lo 2017: 2-3).

Second, the US sought to maintain the existing international order and to secure the United States' place within it (White House 2006; 2015: 7-10; 2017: 25-26). As with the first end, each administration initially saw Russia as a potential partner in achieving this goal, but over time realized that it would not simply fold into the US – led system. Instead, as Russia reacted negatively to US actions, the conflict escalated. Finally, each administration attempted to protect and proliferate American values and its economic model, including within Russia itself (White House 2006: 39; 2010: 44; 2017: 37-38).

Ways

As outlined above, during the period of analysis, the United States sought to achieve three primary goals in its evolving conflict with Russia. While the US remained the most powerful state in the system, it nonetheless faced limitations to its power, increased competition with other states, and changing circumstances at home. As a result, presidential administrations repeatedly reevaluated and adjusted the US approach, even while they largely pursued the same objectives. To understand how the grand strategy played out, in this section I will analyze the ways the US applied its elements of power to achieve its goals in the New Era of Conflict.

Protect the US and its allies

Since the 2001 terrorist attacks, and arguably well before, the United States relied heavily on its military capabilities to achieve its international goals. Indicative of this trend was the US defense budget which far exceeded every other state since the end of the Cold War (World Bank 2019g).

To protect itself and its allies against Russia, the US used its military power in two primary ways. First, through its nuclear weapons and robust conventional military, the US sought to deter Russia from attacking its homeland or fundamental interests. Although the US worked to reduce nuclear stockpiles during the G.W. Bush and Obama administrations, it also invested in updating its nuclear infrastructure and missile defense capabilities, which increased tensions between the two states (DOD 2010: iii-vi; Boese 2008; White House 2002). This trend became more pronounced under the Trump administration, which stepped away from the Intermediate – Range Nuclear Forces treaty, changed the US nuclear investment strategy, and fielded new warheads, specifically in response to Russia’s behaviors (Mehta 2020; DOD 2018a: I-III).

At the same time, the US upgraded its conventional capabilities and acted to offset the perceived growing Russian threat to Europe by stationing a rotating military force in the Baltics and Poland in 2014, after Russia invaded Ukraine (White House 2014a). The US also routinely conducted maritime and air patrols in regions around Russia's border, and reestablished the Navy's Second Fleet in 2018, with the mission to protect shipping lanes against Russian submarines in the North Atlantic and Arctic (LaGrone 2019). Moreover, the US continued to invest heavily in NATO, providing for 22% of its direct funding annually and consistently stationing over 60,000 active duty forces in Europe throughout the period (Béraud-Sudreau & Childs 2018; DMDC 2018; 2016; 2008).

While the military played a principal role in the US grand strategy, its reliance on economic coercion as a foreign policy tool increased substantially during this period (Bandow 2020). Along these lines, the United States' primary approach was to use sanctions to punish Russia and attempt to deter it from engaging in threatening behaviors. Specifically, in 2015 the Obama administration issued four executive orders imposing sanctions on an increasing number of Russian government officials and business owners in response to the Crimea and Ukraine operations. This was followed in 2015 and 2016 by two additional executive orders, later embodied in legislation, through which the US imposed additional restrictions on Russia due to its cyber activities (US Department of State 2017). These sanctions, however, were in addition to those imposed starting in 2012, in response to human rights abuses, Russian-originated organized crime, and the government's support for Assad (CSIS 2020).

Moreover, in addition to measures against Russia proper, the US used a combination of sanctions and other financial means to pressure states in Europe to wean off their heavy dependence on Russian imports. This was done both to protect allies from coercion and exert pressure on Russia’s economy (*The Economist* 2020a; European Union 2019; Collins 2017: 104).

The US also actively used information to warn Russia, counter its propaganda, and shape domestic and global opinions. One of the primary methods was to publicly highlight illicit behaviors, such as Putin’s integration of organized crime into his foreign policy, Russia’s propaganda programs, and its clandestine attacks against Ukraine (White House 2014b; US Department of State 2020b). In addition, recognizing the threat Russia’s information warfare posed, in 2016 the US established the Global Engagement Center to counter “foreign propaganda and disinformation,” with Russia being one of the principle actors of concern (US Department of State 2020a). The US also sought to protect sensitive data while facilitating the flow of other information as a means of defending the homeland, protecting the free market, expanding its influence, and exposing other actors who threatened its security or interests (Lopez 2019; White House 2015: 17-21; 2017: 7-14).

The administrations also invested heavily in technology as the foundation of the Third Offset Strategy, which is designed to deter Russia and China by overmatching their military power through superior conventional capabilities (DOD 2016). These included investments in unmanned systems, cyber capabilities, and artificial intelligence, with the latter’s budget expanding by 40% from 2015 to 2019 (White House 2018b). The attempted overmatch became difficult to maintain, however, as commercially available technologies proliferated to state and non-state actors (DOD 2018b: 3).

In the cyber domain, the US undertook substantial organizational changes and made increasing investments in capabilities to protect US infrastructure, processes, and people from foreign cyber actors' manipulation, intelligence collection, and damage (Statistica 2019e; United States Cyber Command 2020). The resulting campaign had both offensive and defensive elements, involving attacks and cyber espionage operations against Russian troll farms and associated actors (Sanger & Perlroth 2019). At the same time, however, the US Government struggled to implement aspects of its cyber security efforts due to privacy concerns and congressional resistance (Risen 2015).

As during the Cold War, the US used geography to its advantage, deploying military forces to key regions and using the largest Navy in the world to maintain open sea lanes and strong international relationships. It also sought to develop closer associations with states in Russia's near abroad, particularly on NATO's flanks. As a result, NATO expanded by ten countries from 2004 to 2018, and in 2020 listed Bosnia and Herzegovina, the Republic of North Macedonia, Georgia, and Ukraine as aspirant countries (Estonian Atlantic Treaty Association 2020; NATO 2020). At the same time, while the US exploited favorable geography across much of the world, it underinvested in the Arctic, a region that became increasingly important in the ongoing conflict (Werner 2020; Conley 2019).

Maintain the existing international order

As the leader of the international liberal order since World War Two, the United States had an inherent interest in maintaining the status quo and its primacy within it. At the same time, however, the US was slow to identify and act against challenges to the order, particularly in relation to Russia, which it initially hoped to coopt (Polyakova 2019: 2; Stent 2016). As a result, while the Bush, Obama, and Trump administrations invested heavily to preserve the system, their approaches evolved as Russia's rising assertiveness became increasingly apparent.

Consistent with the other goals, the US military played a major role in preserving the international order against perceived Russian interference. Specifically, the US used its military power to support governments and non-state organizations it saw as important elements of the system, often in direct contrast to Russian preferences and operations. Activities included military training, arms sales, and other support to Kosovo, Ukraine, Georgia, and the Central Asian States, as the US courted them for increased access, influence, and resources (USAID 2020b; Cooley 2012; Kleveman 2003). In 2018, for instance, the US provided over $951 million in aid to countries around Russia's periphery, with only 30% for non-military purposes (USAID 2020b). Throughout the New Era of Conflict, the US also deployed units to each of these countries and many others (DMDC 2018; 2016; 2008; 2005).

Moreover, the US used force in or against states that had long-standing relationships with Russia, including Libya, Syria, and Iran. For nearly two decades, the United States also maintained significant although dwindling forces in Iraq and Afghanistan, and it provided episodic support to anti-Assad elements in Syria (Itani 2017). These latter activities placed the US in direct opposition to Russia, which deployed military personnel, aircraft, ships, and Private Military Companies (PMCs) to support the Assad regime. Due to their proximity in Syria, US and Russian forces repeatedly came into contact in the combat zones, and Russian PMCs brazenly attacked US Special Operations Forces (Schmitt, et. al. 2019).

Similarly, in 2011 the US played a leading role in the NATO bombing of Libya, with whom Russia had reestablished relations in 2008 (Fasanotti 2016). This military operation facilitated al-Gaddafi's overthrow and death, and the implosion of the state, which were greatly disturbing to Putin. As a direct outcome, the US and Russia sponsored opposite sides in the Libyan civil war, with the former supporting the UN designated government and the latter its opponent (Souleimanov 2019).

From an economic perspective, the US used both incentives and coercive tools to influence Russia to act in line with the status quo. In the Bush and early Obama administrations, the focus was on encouraging Russia to integrate into the system and accept US leadership (US Department of State 2012; White House 2010; 2006). When Russia took a contrarian stance against many US policies, however, the Obama and Trump administrations shifted to more coercive tools, including sanctions, trade restrictions, aid reductions, and assistance to Russia's adversaries (CSIS 2020; USAID 2020b).

Informationally, the United States engaged in an evolving campaign to shape Russia's behavior and incorporate it into the US led system. While the messaging tended to be positive in the administrations' early stages, it invariably shifted due to Russia's non-normative behaviors (US Department of State 2019b; 2014; 2008). Themes included Russia's violations of other states' sovereignty, its support for the Assad regime, use of largely unaccountable PMCs, and interference in the US and French elections. The US also attempted to counter Russian propaganda through public statements, cyber operations, and judicial action, although its efforts tended to be disjointed, reactive, and of questionable effectiveness (Polyakova 2019: 6-7).

Technology played a considerable role in the United States' attempts to protect the international order and was a key component of its global leadership. Based on World Economic Forum rankings from 2008 to 2018, the US was consistently listed at or near the top for innovation and technological readiness (World Economic Forum 2008: 18; 2013: 21; 2018). Throughout the period, it was also one of the leading OECD countries in terms of research and development investments and a global leader in information and communications technologies, which greatly strengthened its economic position and leverage in cyberspace (Henry-Nickie, et. al. 2019; OECD 2018; 2014: 43).

This technological advantage played three key roles in the United States' efforts to preserve the international order vis á vis its conflict with Russia. First, technology supported the other elements of power, particularly the military, economic, and information components. This was reflected in the Third Offset Strategy, the crucial role US firms played in the global digital economy, and the United States' efforts to maintain an open internet in the face of Russia's attempts to establish state sovereignty (Henry-Nickie, et. al. 2019; DOD 2016; Council on Foreign Relations 2017). Second, the US used technology to develop and sustain relationships with other countries through sharing agreements and exports (US Department of State 2010). Finally, the United States employed its technological superiority offensively to deter and shape Russia's behaviors through increased cyberespionage and cyberattacks against Russia's critical infrastructure (Greenberg 2019).

From a geographical perspective, the US exploited its and other states' favorable locations to expand its reach and exert pressure on Russia. Specifically, the US reinforced its arc of influence around Russia through NATO, its presence in the Middle East, North Africa, the Central Asian region, and its long-standing relationship with Japan. As a result of these military, economic, and diplomatic relationships, the US maintained influence over and access to major maritime chokepoints, critical resources, and other areas of critical importance to the international system. In addition, this network served as a stabilizing counterweight to Russian attempts to shift power, thereby providing an enduring foundation for the United States' post-World War Two order.

Proliferate American values

Finally, a central goal of each Administration was to propagate American values, mainly by using its elements of power to protect human rights, expand economic liberalism, and advance democratic principles. Arguably an enduring provision of US foreign policy since at least the Wilson administration, the goal took on additional emphasis after the end of the Cold War, as some saw the United States' victory as validating liberalism and reinforcing the idea of democracy as a route to international peace (Fukuyama 1992; Russett 1993). Although each administration in the New Era of Conflict attempted to achieve a version of this goal in different ways, presidents consistently pursued it and invested heavily in the process (White House 2017; 2010; 2006).

With regard to Russia, the United States followed an evolving two-pronged approach focused on encouraging or coercing its government to adopt internal reforms while also taking aggressive action toward other states with which Russia had long-standing interests. While these latter efforts were not always targeted at Russia *per se*, they nonetheless directly influenced how its foreign policy executive (FPE) perceived the international environment and associated risks to its security. From the Russian FPE perspective, US efforts to propagate its values played a fundamental role in the ongoing conflict (Bartosh 2018; Russian Federation 2015: 9).

Toward this normative goal, the US applied its elements of power to directly and indirectly support democratic movements and governments in the Middle East, North Africa, South America, and the Central Asian States. Most disconcerting for Russia was the real and perceived aid the US provided to burgeoning democratic movements in states such as Ukraine, Egypt, Tunisia, Iran, Georgia, Kyrgyzstan, Venezuela, and Russia itself (Bērziņa 2014). Through these and other programs, the US exploited its global access to directly challenge Russian influence and attempts to gain geographical power by developing relationships in important strategic locations.

Moreover, the US periodically intervened militarily to protect human rights, including in Libya and Syria, and provided military, economic, and technological support for other states and democratic movements (Stockholm International Peace Research Institute 2020; Carpenter 2019). In addition, through trade agreements, information campaigns, and military operations, the US actively attempted to preserve economic liberal norms and expand their influence. This included programs such as Radio Free Europe, name and shame campaigns, Freedom of Navigation Operations in strategic waterways, sanctions against violators, technology sharing with likeminded states, and influencing international institutions' decisions on who should become members (Congressional Research Service 2020; Talbott 2006).

The US Administration for International Development (USAID) contributed significantly to this process, as it expended an average of $47 billion per annum for financial assistance, educational programs, election oversight, and other norm-related services during the period of study (USAID 2020a; 2020b). In addition, the Departments of Defense, Justice, Treasury, and State, also dedicated resources to encouraging the development of democratic institutions, rule of law, and liberalized economies (DOD 2020; Department of Justice 2020).

While the US goal was generally in line with enduring norms, its approach expanded over time and was seen by some as a form of warfare (Bandow 2020). For Putin this was particularly disconcerting as the US consistently listed Russia as a human rights violator and used economic sanctions and information campaigns in an attempt to force changes (US Department of State 2018; 2013; 2008). This created enduring, fundamental tensions between the states that predated the conflict and greatly impacted its evolution.

Cyber capabilities played an important role in US efforts to achieve this goal, particularly in its support for information operations. Specifically, many of the United States' efforts to encourage freedom of the press and democratization relied heavily on the internet, including traditional platforms, such as Voice of America, Radio Marti, and congressionally funded Radio Free Europe. The US also launched extensive social media campaigns to propagate its narrative and gain direct access to people who lived in states with government-controlled press.

Analysis of US Grand Strategy

Based on the above, it is evident the US followed an evolving but generally consistent grand strategy relating to Russia during the period of study. To provide the foundation for a model of the US approach, in this section I will synthesize the above using the neoclassical realist framework outlined in previous chapters. The results are reflected in Table 5, below.

Table 5: US Approach to International Conflict in the NEC

Variables Elements	FPE Perceptions	Ability to access & employ resources	Strategic Culture
Military (nuclear & conventional forces, security assistance)	Deter Russian FPE & shape perceptions by deploying forces to contested regions, upgrading nuclear arsenal, withdrawing from agreements, & deploying missile defenses. Pursue 3rd Offset Strategy. Build & sustain alliances. Maintain largest & most advanced military in the world.	Build relationships through arms sales, exchanges, & exercises. Directly intervene in states of Russian strategic interest, coerce its long-standing partners, & assist its adversaries. Enhance military relationships to offset Russian access & influence.	Use conventional & nuclear enhancements & deployments to impact cost-benefit calculus in favor of US goals. Deploy forces to undermine Russian security, deter direct attack against allies & strengthen relationships.
Economic (aid, trade, export controls, sanctions, rewards)	Use sanctions to strain Russian economy, challenge its decision-making, & deter aggressive actions. Provide aid to countries in Russia's near abroad & other strategic regions to gain or sustain influence. Use dominant position in global financial system.	Manipulate oil production to weaken income on main commodity. Impose sanctions on exports, businesses, & oligarchs to undercut the economy & Putin's popularity. Use aid & sanctions to encourage other states to move away from Russian petroleum products & decrease its influence.	Use sanctions, trade relationships, & defense investments to weaken centralized power structure.
Information (exchanges, press releases, speeches, diplomacy, influence in forums)	Use international bodies, diplomatic channels, & press statements to influence allies & others to support the US & undermine Russian influence. Counter Russian overt propaganda, active measures, & espionage.	Exacerbate domestic tensions to undermine confidence. Expose coercion to undermine trade & relationships. Expose crime, corruption, & oligarchs to undercut popular support, relationships, & businesses. Counter attempts to gain domestic information control.	Undercut secretive government & self-image by exposing deception, corruption, & human rights abuses. Spread narrative on human rights & free trade to demonstrate higher principles. Conduct espionage to understand & exploit FPE plans & operations.
Technology (export limitations, advanced R&D, investments)	Pursue technical superiority across government & private sectors. Invest heavily in AI, ICT, missile defense, & space R&D. Routinely demonstrate tech capabilities.	Impose data export limitations & sanctions on technology. Counter attempts to create sovereign internet & domestic information control.	Use R&D & advanced capabilities to shift Russian risk calculus.
Geographical (open ports, proximity, & relationships)	Challenge perceptions by demonstrating US global reach & geographic security.	Build relationships to offset Russian access & influence in critical regions.	Use global reach to challenge Russia's perceived sphere of influence, great power status, & attempts to shift power.
Cyber Capabilities	Counter Russia's operations to deter assertiveness & undermine activities. Disseminate information globally to undermine FPE sense of opportunities, security, & control.	Deny Russia operating space, opportunities, & information. Use cyber to access Russian populations to undermine domestic information control & support for Putin.	Information operations to undermine secrecy, control & hierarchical decision-making. Create challenges & exploit vulnerabilities in cyber domain.

Russia's Grand Strategy in the New Era of Conflict

An Overview

Although Russia experienced two leadership changes during the 2007 – 2018 period, they were largely *pro forma* position shifts driven by constitutional mandates against a president serving more than two sequential terms. Thus, while Vladimir Putin became prime minister in

2008, with Dmitri Medvedev as president, in 2012 they swapped seats, thereby allowing Putin to step aside for a mandatory waiting period while still retaining power. This tandemocracy endured thereafter, with Putin reappointing Medvedev to the prime minister position again following his reelection 2018 (Ryabov 2008).

While there were some apparent variances in Russia's grand strategy, with Medvedev initially taking a more conciliatory approach toward the West, in practice the dissimilarities were superficial (Duncan 2013; Monaghan 2011: 1-2). In addition, although some observers saw a potential conflict brewing between the two leaders, it did not openly manifest (*The Economist* 2011; Weir 2011). In effect, therefore, the swap in positions had no substantive impact on policy, with Putin maintaining continuity in leadership (Tayler 2008).

As a result, during this time, state control was consolidated in Putin's hands and he became a central and enduring figure in Russia's government, to the point where some saw him as synonymous with the state. This cult of personality, which was carefully cultivated by Putin and his inner circle, was aptly described by Vyacheslav Volodin: "as long as there is Putin – there is Russia, there is no Putin – there is no Russia" (*Lenta* 2014).

In view of the above, scholars largely agree that Russia followed a consistent, evolving grand strategy throughout the time period (Herspring 2009: 156-157; Gurganus 2018; Rumer 2018). This approach is captured in the Ministry of Foreign Affairs' Concept of Foreign Policy (CFP), which reflects a sense of Russian exceptionalism and concerns about the West's perceived unilateralism, support for popular revolutions, and competitiveness, which it blames for much of the global instability (Russian Ministry of Foreign Affairs 2016; 2013; Saivetz 2012: 375). To counter these negative developments, Russia actively worked over the decade to reverse the West’s effects around the world, particularly by attempting to undermine US power and change the international regimes that supported it.

Ends

As with research on the Soviet Union during the Cold War, locating authoritative documents reflecting Russia’s decision-making and priorities presented a challenge. Although the Russian government became more open after the Cold War, it nonetheless still valued secrecy and deception as key tools for maintaining state security (Bouwmeester 2017: 125-126). Thus, records were not only difficult to locate but they also were of suspect accuracy.

To address these challenges, I used two main types of sources to support my analysis. First, I used government documents and speeches where they were available. To mitigate the risks of propaganda, I interpreted these sources in context with the government’s actual behaviors. Second, I used academic literature and other secondary sources to support the primary materials or fill in gaps where it was not available. In the process, I used these references both as backstops for the government documents and to gain insights into Russian policies and actions. Taken together, these sources provide a comprehensive view of Russia’s grand strategy.

Based on these data, I found that throughout the period of study Russia followed a consistent although evolving grand strategy, with three interrelated goals (Monaghan 2018). First, the highest priority was to protect Russia. This, however, was not limited to the homeland within the state’s internationally recognized borders, but also greater Russia, which includes Russian speaking populations and the near abroad (Roberts 2017; Adomeit 2018; Russian Federation 2015: 6). In addition, for Putin and his inner circle, this invariably meant protecting their hold on power (Gurganus 2018: 11). Second, Putin sought to rebuild Russia’s status on the international stage and return its national pride to pre-collapse levels (Clark 2019: 229-231; Stent 2018; Freiré, Maria 2009: 128-129; Russian Federation 2015: 6). For Putin, the collapse of the Soviet Union and its aftermath was "a major geopolitical disaster of the Century" (Putin 2005). As a result, he attempted to reverse its negative effects and prevent a similar situation from recurring (Rumer 2018). Finally, and closely related to the previous goals, Russia attempted to change the US dominated international order, which Putin saw as dangerous for global security and as an unnecessary constraint on Russian actions (Putin 2007; Clark 2019: 229-230).

Collectively, these ends guided Russia's international behavior. To understand how Russia implemented its grand strategy, and therefore how it engaged in international conflict, in the next section I will analyze the ways the Putin regime used the state's elements of national power in its ongoing struggle with the US.

Ways

From 2007 to 2018, Russia attempted to change the dynamics of international power and to create a more favorable environment in which to protect its interests. To accomplish this, Putin used traditional and non-traditional approaches that, for many Western observers, seemed extreme in context with normative standards of the post-Cold War world. In the process, Russia invaded sovereign states, supported violent insurgencies in break-away provinces, assassinated foreign adversaries with poison and nuclear isotopes, conducted extensive cyberattacks against others' critical infrastructures, meddled in foreign elections, and threatened the United States with nuclear annihilation.

Taken individually, these events seem to be surprising and aberrative overreactions to questionably provocative behaviors. However, viewed comprehensively and in context with the

Russian perspective outlined above, Putin's approach represents a novel application of the state's capabilities against the US, which he saw as an overextended and meddlesome hyperpower. The ways the Russian Foreign Policy Executive sought to accomplish its goals are outlined below.

Protect Greater Russia

For Vladimir Putin, Russia is not limited to its recognized international borders, but reaches well beyond, to include other states' territory arcing from the Baltics to the Central Asian States. A key component of this Greater Russia are the compatriots, or Russian speakers, within many of the post-Soviet states and for whom Moscow claimed sovereign responsibility (Pigman 2019: 24-25; Kallas 2016: 5-6; Russian Federation 2015). To protect this expansive version of Russia from perceived ongoing attacks by the West and prevent its integration into the larger European Union, Putin employed all the state's elements of power, often in surprising ways (Roberts 2017: 47-48; Snyder 2015: 703-705). This was particularly true of the military, which Russia used to offset US influence in its near abroad in four general ways.

First, the Russian military conducted attacks on neighboring states, such as its invasion of Georgia in 2008. This operation, which involved an estimated 25,000 ground forces and 300 combat aircraft, was a wholesale attack unlike anything Europe had experienced since the end of the Cold War (Cohen & Hamilton 2011: 10-11). In addition, to exacerbate ethnic tensions and divide Ukraine after the Maidan uprising, in 2014 Putin ordered the Russian military to conduct clandestine operations against the Crimea and the Donbas regions of the country. Despite Russian claims to the contrary, its military was heavily involved, with special operations conducting the Crimea annexation and thousands of soldiers, modern armor, rockets, and artillery crushing Ukrainian defenses to reverse sponsored separatist setbacks (Fox 2019: 2-9;

Kofman, et. al. 2017: 44). To support these operations, Russia also conducted extensive cyberattacks on communications, electrical power, government websites, and other critical infrastructure, some of which rippled across the globe, inflicting billions of dollars in losses to industries and governments (McQuade 2018).

Second, Russia actively employed its military in an indirect role to shape the near abroad in its favor. Emblematic of this approach were the so called frozen conflicts, in which Russia used military assistance to preserve and embolden separatist movements in Georgia, Moldova, Armenia, and Azerbaijan, thereby holding the disputes in a perpetual hiatus (Grossman 2018: 51-53). The resulting instability provided Russia with a mechanism to coerce victim states into shifting away from European integration and recognizing Russian interests inside their borders (Blank 2008a: 23). Moreover, extending beyond large-scale operations, Putin ordered the assassination of perceived traitors using poison, nerve gas, and radioactive isotopes in London and Berlin. Taken together, these first and second military uses served Russian interests by generating fear and demonstrating a willingness to act against its perceived enemies anywhere in the world, while also staying below the threshold of an unacceptable US or NATO response (Levick 2018).

Third, starting in 2007 Russia greatly expanded its military deployments, long range patrols, and exercises. Specifically, in 2007, Russia resumed long-range bomber patrols, sending aircraft into the Arctic, NATO periphery, South America, and the Gulf of Mexico (Aliyev 2019; Russian Ministry of Defence 2018a; Nicoll and Delaney 2015). This pattern is also reflected in its naval ship, maritime reconnaissance, and nuclear missile submarine deployments, which increased significantly in the Arctic, an area of increasing military and economic importance

(Mikkola 2019; Norwegian Intelligence Service 2019: 22-25). Emphasizing this point, in 2007 Russia used a submarine to plant its flag on the submerged seabed of the North Pole (Kremlin 2007). On the ground, Russia used large troop formations as a warning to other states, and the Russian military participated in multiple international exercises, including combined events with the Central Asian States, Pakistan, Laos, India and China (Russia Ministry of Defence 2019; Defense Intelligence Agency, hereinafter DIA 2017). Collectively, these actions served Russian interests by training personnel, providing information about US and allied responses, and sending a powerful message against the West's incursions into its perceived sphere of influence (Nicoll & Delaney 2015).

Fourth, Russia employed it military as a deterrent against US or allied attacks on its territory. This approach is evident in the priority Russia placed on updating its nuclear forces, including building new strategic ballistic missile submarines, modernizing its land-based intercontinental ballistic missile force, and enhancing associated command and control systems (Rumer 2019: 4-5; Office of Naval Intelligence, hereinafter ONI, 2015: 17). As a result, in 2018 Russia maintained over 1400 strategic nuclear warheads as part of its land, sea, and air-based triad (Nuclear Threat Initiative 2019). In addition, Russia was not shy about advertising these capabilities, as reflected in a state news broadcast in 2014 that "Russia is the only power capable of turning the United States into radioactive dust" (Ennis 2014).

From a conventional standpoint, Russia also greatly enhanced its defensive systems through the deployment of land-based missiles capable of reaching 1000 nautical miles out from its maritime boundaries, encapsulating vast areas of Europe, the arctic, northern Pacific, Japan, and Alaska (ONI 2015: 3-4). Taken together, these nuclear and conventional forces provided

Russia with a combination of capabilities with which to inflict severe damage on any would-be attacker and the flexibility to escalate rapidly so as to set the foundations for de-escalation and negotiations in its favor (European Union 2017: 15-16).

Economically, Russia attempted use it ties with Western and Eastern European countries as leverage in its efforts to push them away from the US sphere of influence. One such approach, was to highlight the benefits of Russian – European integration, which the Russian Foreign Secretary echoed in 2014 when he commented on the need for a "common economic and humanitarian space from the Atlantic to Pacific Oceans" (Lavrov 2014). At the same time, however, Russia used its vast energy resources and European dependence thereon as a weapon against states in the near abroad and Western states (Collins 2017: 104; United States Congress 2018: 17; Blank & Kim 2016). In addition, Russia attempted to increase influence with states, and pull them away from the US, through the lure of oil-related infrastructure development, military basing, and cultural connections (Freiré 2009: 130-134).

Russia also relied heavily upon its information power to protect its perceived sphere of influence. The compatriot policy and Putin's apparent willingness to use military force to implement it provided a foundation for Russia's activities in the Baltics and Central Asian States. Building on this, Putin used active measures to exacerbate ethnic and political divisions throughout these regions. Beyond the 2007 Estonian riots, post-Soviet states witnessed the increasing use of complex propaganda campaigns involving social media, *Russia TV* (RT), public speeches, government-sponsored organizations, and human-based networks to spread manipulated stories and blatant falsities in an effort to create confusion, counter criticism, and undermine target states' governance (Senate Report 115-21 2019: 37-40; Lankina & Watanabe 2017: 1526-1527; Bērziņa 2014: 19). At the same time, Russia used similar approaches to enhance its domestic and international image, as a comparable offset to the apparently corrupt and exploitive US (Kremlin 2014). These techniques not only supported Putin's goal of increasing Russia's status on the world stage, but they also influenced compatriot populations to identify with Mother Russia and to serve their protector's interests (Thomas 2015: 384).

These techniques, however, were not limited solely to Eastern Europe, as Russia also used its information power in an attempt to divide NATO, undermine European integration, and attack US social cohesion (Seldin 2019; United States Congress 2018: 1-35; Snyder 2015: 703). While similar to the active measures employed by the Soviets during the Cold War, these activities' reach and scope were greatly increased by cyber technology since Russian propagandists no longer had to rely on the news media to pick up the story line. Instead, the Russian Internet Research Agency used groups of trolls, or government directed social media users, to publish unfiltered information directly on social media platforms for consumption by targeted audiences (Gurganus 2018: 12-13; Graff 2017a). Through these operations, Russia used technology to magnify social tensions over issues such as race, gun control, elections, and women's rights (Thompson & Lapowsky 2018; Fritze 2017; Ioffe 2017). As the former director of the US National Security Agency stated, Russian cyber operations during the 2016 presidential election allowed it to perpetrate "the most successful covert influence campaign in recorded history" (Nye 2018).

In addition to its influence efforts, Russia relied heavily upon spies, augmented by specially designed communications devices and other capabilities to gather and pass information to intelligence agents (Southern District of New York 2010: 4-5). Through these operations and extensive cyber espionage activities, Russia collected data about US infrastructure, defense programs, and social conditions, and stole information from government and industry sources to help its struggling economy, facilitate military modernization, and support potential cyberattacks (DNI 2019: 5-6; 2018: 8-9).

Technologically, Russia focused on modernizing its military, as reflected in the advanced capabilities it employed during operations in Ukraine and Syria and its long-range, hypersonic anti-access, area denial systems (DIA 2017). In addition, Russia invested heavily in offensive cyber resources that allowed it to attack, infiltrate, and manipulate networks and critical infrastructure in the US and allied countries (US Department of Homeland Security 2018). In the process, Russia became one of the most advanced and active cyber states in the world, perpetrating at least eighty-two *detected* cyber events from 2005-2020, with twenty-two targeting the United States (Council on Foreign Relations 2020). At the same time, Russia adopted defensive measures, including pursuing the concept of a “sovereign internet,” or runet, that could be isolated from overseas servers, ostensibly to prevent the US from using Russia’s dependency on external capabilities as a point of attack or economic leverage (Kremlin 2019c).

Finally, from a geographical perspective, Russia used its proximity and associated historical, cultural, economic, and institutional connections with other states to reinforce the Greater Russia narrative and exert influence (Babayan 2015: 443). Collectively, this approach created significant problems for many of the states surrounding Russia, as it exploited these relationships to coerce and coopt their governments and populations (Grigas 2012).

Moreover, Russia used its proximity to Afghanistan as an attempted leverage point with the US and NATO. Specifically, as the allies were facing challenges due to attacks on their logistics lines that passed through Pakistan, Russia opened its territory for the transportation of materials from Europe. This route, called the Northern Distribution Network (NDN), was longer than the Pakistani lines, but much safer. However, in 2015, Medvedev ordered that the Russian segment of the NDN be closed due to degraded relations between Russia and NATO following the Crimea and Donbas operations (Daly 2015).

Restore Russia’s Great Power Status

Closely related to its goal of protecting Russia’s near abroad were Putin’s attempts to restore the state’s international status. Driven by a sense of post-Cold War victimhood and tragedy, this end played a substantive role in Russia’s identity as a great power and was a key driver behind its domestic and international behaviors (Stent 2018; Roberts 2017). While it is unclear by what standards Putin measured great power status, it is evident that he believed Russia had been unjustly sidelined in international affairs and deserved to be recognized as a major player on the world stage (Reshetnikov 2018; Stoner 2014).

As the element most associated with a great power, the military played a critical role in Russia’s international image. Due to this, Russia invested heavily in developing a modern, professional, and capable force that it employed in highly visible ways around the world. This was aptly demonstrated in Russia’s operations in Syria, in which it showcased the use of bombers, fighter aircraft, drones, submarines and surface ships to strike targets from multiple launch sites, including the Mediterranean and Caspian Seas (Russian Ministry of Defence 2018b; Chandler 2015; Russian Ministry of Defence 2015).

In addition, Russian long-range aviation flights, much publicized ballistic missile tests, international exercises, technological developments, and explicit nuclear threats served to reinforce this great power narrative (Kremlin 2019f). While the Russian military was far smaller than the United States', and therefore did not have the capacity to engage in an extensive campaign over a large area, in 2018 it likely had a significant advantage over NATO in Europe and was capable of inflicting severe costs on adversaries nearly anywhere on Earth (Boston, et. al. 2018). This was a message Putin wanted the world to hear.

Military spending and international relationships, however, could not stand alone without the economic power to support them. Recognizing this, Putin employed a cautious and partially successful economic strategy designed to provide stability, low debt, and moderate growth in the face of lower oil prices and sanctions (Miller 2018). At the same time, Russia worked to increase its foreign trade, leading to 218 partners and a consistently positive trade balance. Moreover, Russia attempted to build relations with states around the world through military engagements and arms sales that were second only to the United States in volume (Stockholm International Peace Research Institute 2020). At the same time, however, Russia's overall trade dropped during the period of study and petroleum products represented a substantial portion of its overseas sales (World Bank 2019k).

As with its first goal, Russia also relied heavily on information to portray itself as a great power. From ceremonies surrounding the 2014 Sochi Olympics to Putin's speeches, Russia worked diligently to establish its status on the world stage and convince domestic audiences of the same (Gurganus 2018: 13; Putin 2015; Persson & Petersson 2014). To support this narrative and validate its greatness, Russia routinely highlighted its role in defeating Nazi Germany while reinterpreting the Molotov – Ribbentrop Pact and other states' culpability in the outbreak of World War II (*The Economist* 2020b; *RT* 2018; Walker 2018). The Russian government also attempted to recast the 1980s war in Afghanistan, including denouncing official statements made by Gorbachev in 1989 expressing regret for the invasion (Interfax 2018; Kara-Murza 2018).

Moreover, Russia used cultural centers in the United States to strengthen relationships with the American people and demonstrate Russia's contributions to the world (Russian Cultural Centre 2020). While Russia advertised these centers as platforms for enhancing understanding of its history and culture, some within the US claimed they recruited and employed spies (Simpson 2013).

Regardless of whether the cultural centers played such a role, however, Russia nonetheless engaged in extensive human and cyber-based espionage to steal US industrial and military secrets to support its return to great power status (DNI: 5-6; 2018: 8-9). In addition, it relied heavily on cyber trolls to spin social media posts in Russia's favor and bots to proliferate deceptive messages or other content to overwhelm counternarratives (Gurganus 2018: 12-13; DIA 2017: 40). As part of the deception cycle, Russia used hacking operations to feed the trolls and state – sponsored media, such as *RT* and *Sputnik* news, as dissemination mechanisms (Popescu 2018).

Moreover, to offset what it perceives as the imposition of US ideals on the world, Russia emphasized its traditional values and institutions domestically and internationally (DIA 2017: 15; Russian Federation 2015: 21). One of Russia's key tools in this effort was the Russian Orthodox Church, which had a close relationship with the Kremlin, its military, Greater Russia, and other important regions (Russian Orthodox Church 2020; Adamsky 2019).

From a technological perspective, Russia trumpeted its past accomplishments while also attempting to develop advanced space, cyber, and electronic warfare capabilities (DIA 2019: 25-29; Rodgers 2019). In addition, Russia dramatically increased investments in artificial intelligence research, which Putin emphasized as the key to world leadership and Russia's place within it (Kremlin 2019b; Polyakova 2018; *RT* 2017). Russia also led in the development of hypersonic missiles, such as the Avangard system, which Putin claimed could defeat US antiballistic missile capabilities by traveling at 9 time the speed of sound (Kremlin 2019d). As part of this effort, Russia attempted to develop nuclear powered and unmanned air and subsurface systems with unlimited range and endurance, although the capabilities suffered significant setbacks (Kremlin 2019f; Webb 2019). Collectively, these capabilities were focused on offsetting US advantages through unconventional approaches and demonstrating Russia's status as an advanced state.

Similarly, Russia touted its geographical greatness, from its vast size to its rich natural resources (Kremlin 2019f). An important part of this status was Russia's extensive arctic region, which Putin saw as a portent of global influence and a source of national pride (Rotnem 2018; Kremlin 2017a). As such, Putin reinforced Russia's position as an Arctic power through military maneuvers, public displays, and official statements. In addition, from Norway's Spitsbergen Island to the Japanese claimed Kuril Islands in the North Pacific, Russia reasserted claims and took steps that other nations saw as aggressive efforts to reinforce sovereignty over contested territory (Roberts 2010: 957-959; Ministry of Foreign Affairs of Japan 2017).

Revise the international order

Of Russia's three goals in the New Era of Conflict, the most controversial is its purported effort to revise the international order. According to Russian statements, Putin was not attempting to change the underlying norms and structures but instead wanted to restore balance to a system that had become misshapen due to the United States' overwhelming dominance and its aggressive use of that power to undermine state sovereignty (Kuchins 2015: 118-119; Russian Federation 2015; Putin 2013). For many other nations, however, Russia's actions were not designed to achieve a benevolent restoration of some harmonic system but rather represented revisionist attempts to exert its unwelcomed influence in former Soviet spaces and exert its power on the global stage, often through coercive and underhanded means (EU 2017: 22-25; Stronski & Himes 2019: 1-2).

Regardless of which intent is attached to Russia's grand strategy, it is nonetheless clear that Putin was actively attempting to change the existing order to one that was more beneficial to Russia's interests and more closely resembled the system that existed before the Soviet Union collapsed. In the process, Russia applied many of its means in ways that clearly contravened long standing international norms. Thus, despite the purportedly lofty goals, it is evident that Russia's grand strategy was heavily influenced by its conflict with the United States and its associated desire to change a system that was led by its principal adversary (Stent 2018).

To accomplish this, Putin used every means to offset US advantages and redefine the balance or even meaning of power on the international stage (Clark 2019). Employing what commentators labeled hybrid warfare, reflexive control, or the Gerasimov model, Russia used a combination of clandestine and overt military force, propaganda, deception, cyber operations, and proxies to coerce, influence, or manipulate other states' governments and their populations (Kasapoglu 2015; Giles 2016).

Like with Russia's other strategic goals, the military played an important role in this process, as Putin used it in direct and indirect ways to challenge US power while staying below the threshold of armed conflict (DIA 2017: 41; Russian Federation 2015). From overt attacks on Georgia to clandestine operations in Crimea, the Russian military provided Putin with a powerful tool with which to create strategic dilemmas for the United States and its NATO partners, particularly since it posed a formidable foe with whom armed conflict would be disastrous. In addition, since many NATO members preferred to maintain positive relationships with Moscow, the alliance faced the real risk of internal divisiveness, which was a key Russian objective in its efforts to revise the international order (EU 2017: 21-23).

Russia also used its military to challenge US power outside of Europe, particularly in the Middle East and North Africa. From its overt use of force to backstop the flagging Assad regime to support for the heavily sanctioned Iran, Russia acted to directly counter US efforts to shape the region in its interests. In addition, Russia used Private Military Companies (PMCs), such as the Wagner Group, to enforce domestic order, support its military, and extend its power overseas (Østensen & Bukkvoll 2018: 22-28). Unlike US contractors, however, Russian PMCs often were not officially recognized, and they operated semi-autonomously, at times engaging in combat operations to support private businesses (Spearin 2018: 67-68). Through such PMCs, Russia expanded its military footprint in Syria, Ukraine, Libya, Sudan, the Central African Republic, and other locations, while simultaneously maintaining a veneer of deniability (Marten 2019: 181). Moreover, the PMCs in Syria directly attacked US forces, although Russia denied any responsibility for the exchange (Schmitt, et. al. 2019).

In addition to its military forces and PMCs, Russia used its robust arms market and associated military technical assistance as mechanisms for gaining access to and influence with key states, including China, Egypt, India, Libya, Turkey (Norwegian Intelligence Service 2019: 36; Souleimanov 2019; Kozhanov 2016). These relationships presented Russia with opportunities to gain income and influence with customers who were provided with advanced military capabilities and international empowerment (DIA 2017: 19; ONI 2015: 15; Freiré 2009: 133).

Finally, Russia sought to establish the Collective Security Treaty Organization (CTSO) to compete with NATO. Established in 2002 as an outgrowth of a 1990s treaty among the Commonwealth of Independent States, the CTSO is a collective security organization that includes Russia, Armenia, Belarus, Kazakhstan, Tajikistan, and the Kyrgyz Republic (Organization of the Treaty of Collective Security 2020). Although CTSO has been compared to NATO in the past, and there are some resemblances, it nonetheless is much less capable, smaller in size, and lost members rather than growing since it was established (Barany 2007: 188).

Economically, Russia attempted to alter the international order in three primary ways. First, as discussed above, Russia used its exports, particularly arms sales and energy, to influence state decision making and exploit divisions among NATO partners. This was most recently on display with Russia's 2019 arms sales to Turkey, which exacerbated ongoing tensions within the alliance (NATO 2019b; Russian Ministry of Defence 2018c). Second, Russia employed state run businesses, organized crime, and intelligence operatives to infiltrate states' communities and governments (Blank 2008b: 227-229). Russia then used this access to influence policy decisions, confound decision making, and exploit social division.

Finally, Russia worked to create international institutions to parallel those run largely by the West as offsets to US leadership. One such entity, The Shanghai Cooperation Organisation (SCO), was established in 2001 to improve political, economic, scientific, and other forms of cooperation among its members and provide the foundation for the creation of a "democratic, fair and rational new international political and economic order" (SCO 2020). Similarly, Russia led the creation of the Eurasian Economic Union (EEU). This organization, which in 2020 included Armenia, Kazakhstan, Belarus, Russia, and the Kyrgyz Republic, was established in 2014 to strengthen the members' economies, solidarity, and cooperation (EEU 2014). Russia's leadership and the speed at which it sought to establish the EEU, however, raised questions about Putin's intentions and its role as a veneer for Russian regional hegemony (Sadri 2014: 554).

Furthermore, Russia attempted to develop stronger economic relationships with countries outside the Soviet sphere and to provide alternatives to the US – led monetary system (Russian Federation 2015, 24; Tsygankov 2011: 35; Roberts 2010). To achieve this, Putin worked with Russia's fellow BRICs and other states to lessen the role of the US dollar in their transactions and to create alternative mechanisms to reduce the dollar's utility in exerting economic pressure (*The Economist* 2020c; Kremlin 2019g). Along these lines, Russia supported China's development of its Belt and Road Initiative (BRI) as an enabler for its oft stated goal of achieving Eurasian integration (Kremlin 2019a). While the BRI offered some benefits and provided an economic balancing mechanism against the US, the close partnership also created the risk that Russia would become a subservient power to China's interests (Sakai 2019). As such, while courting China, Putin attempted to maintain a delicate balance in which his efforts to change the international order did not undermine Russia's security or place on the international stage.

As with its other goals, information power played a major role in Russia's attempts to alter the international system. Through presidential statements and covert active measures, Russia conducted a broad-based information campaign against US global leadership. This is evident in Putin's speeches at various forums in which he decried the United States' duplicity and arrogance, arguing that the US was undermining the foundations of the UN Charter and security writ large (Kremlin 2019f; Kremlin 2015; Kremlin 2014). Ironically, and by design, Putin often delivered these speeches while Russia was simultaneously engaging in behaviors that ran directly counter to the principles he claimed to uphold.

In addition to these public statements, Russia also used indirect methods to revise the international order. These included overt and covert activities, such as attempting to develop closer relationships with key NATO countries, infiltrating Russian populations in Europe, and conducting targeted cyber and media based deception operations designed to undermine US political integrity and soft power (Greenberg 2020; Yegin 2019; Banks 2017: 1487). The challenges these and other actions posed were aptly demonstrated in Russia's 2007 Estonia cyberattacks and its operations in Ukraine, as they presented NATO with difficult decisions. In both situations, Russia's approach created confusion, was sufficiently deniable, and raised such dire political, economic, and military risks that NATO was divided and unable to respond until after the damage was done (EU 2017: 21-23; NATO 2016). While Russia was not always successful, and at times its activities backfired, these operations played a key role in its efforts to challenge the global order while controlling escalation (DIA 2017: 38; EU 2017: 23).

Technologically, Russia employed many of the same techniques it used to achieve its other goals, including a heavy reliance on cyber operations. In addition, as a means of influencing future international business models, Putin demonstrated personal interest in a Russian-produced cryptocurrency and its associated blockchain, Ethereum (Kremlin 2017). While cryptocurrencies were nascent and problematic due to their misuse and volatility, blockchains held the potential for dramatically changing how businesses and governments conduct financial transactions and maintain records (Mavadiya 2017). Gaining an early foothold in the technologies and their regulation placed Russia in a good position with which to influence their development and take advantage of future opportunities as they arise.

Finally, from a geographical perspective, Russia attempted to use its proximity as well as its close historical and cultural connections with the Baltics, Ukraine, and the Central Asian

States to undermine existing international relationships and offset US access. While this backfired in the first two locations, Russia was able to pressure some of the Central Asian States into removing or reducing US presence in the region (Freiré 2009). Furthermore, by exploiting its proximity to separatist regions, Russia was also able to discourage Georgia and Moldova from building closer relationships with Western Europe and NATO (Grossman 2018).

As with the other goals, Russia's arctic region played an increasingly important role in its attempts to alter the international order. Specifically, during the decade, Putin substantially increased investments in the arctic with the hope of shifting over 80 million metric tons of shipping per year to routes predominantly through its Exclusive Economic Zone (Kremlin 2019e). This not only promised billions of dollars in increased economic benefits, but, depending on its scope of success, also could increase Russia's geostrategic importance relative to the U. S.

Throughout, cyber technology enabled many of the operations across the elements of power and provided Russia with both offensive and defensive capabilities that it used widely. Most critically, Russia exploited the United States' heavy integration of cyber technologies and its open society to inflict direct harm to its domestic integrity and international security. These activities included limited attribution hack and release operations and the dissemination of deceptive materials that created confusion, exploited divisions, and undermined confidence in information sources and the associated decision-making processes.

In addition, Russia conducted cyber espionage to steal technology that supported its military modernization, technological advancements, and economic reforms. These activities also provided access to critical infrastructure in the US and its allies' territories, which Russia used to plan and conduct sabotage operations. Thus, through cyber technology, Russia was able to gain access to locations to which it otherwise would have been prevented due to geographical and physical security restrictions. Collectively, these advanced cyber capabilities and Russia's assertive use of them, created direct, clandestine effects that had significant negative impacts on US security and raised fundamental questions about its power and the associated metrics.

Analysis of Russia's Grand Strategy

Collectively, the above demonstrates that, over the decade, Russia engaged in a concerted grand strategy designed to protect its sphere of influence, restore its due place on the world stage, and change the international order to the detriment of US power. While the means and ways evolved with developments at home and abroad, Russia stayed true to these basic goals.

In the process, Putin exploited four US vulnerabilities to limit the United States' ability to respond to actions that impinge on its interests. First, Russia's nuclear and conventional capabilities and policies on first use and escalation were deterrents against US or NATO. In this way, they served a holding function that limited where and how adversaries could respond without engendering an unacceptable response. Second, Russia used active measures to exacerbate internal US and NATO divisions, create confusion, and exert political pressure on decision-makers. Similarly, Putin's use of limited attribution approaches challenged decision-makers' ability to sufficiently demonstrate Russian culpability, particularly in the face of political, economic, and security concerns raised by a US or NATO response. Finally, Russia chose options that fell within areas of uncertainty in the West's legal and normative structures. Taken together, these four pincers created strategic dilemmas that severely limited the United States' ability to respond in ways that seriously threatened Russia's goals and they raised questions about the meaning and use of power in the Twenty-First Century. The below table examines Russia's strategy using the neoclassical realist intervening variables.

Table 6: Russia's Approach to International Conflict in the NEC

Variables Elements	FPE Perceptions	Ability to access & employ resources	Strategic Culture
Military (nuclear & conventional forces, security assistance)	Modernize & advertise nuclear triad to deter US. Reform conventional military to create smaller, more lethal force. Conduct nuclear capable patrols & other deployments to showcase capabilities & undermine US security & enhance own image. Support proxies that directly compete with the US in key areas. Use overt & covert military & PMCs to attack adversaries, expand power, assassinate critics, & complicate US & NATO decision making & operations.	Use proxy forces to undermine US access to strategic areas. Threaten US partners & exploit NATO divisions through overt & covert operations. Attack non-NATO partners directly or thru proxies & frozen conflicts. Use arms sales to gain access & influence in key countries to create strategic dilemmas for US relations & force employment. Establish alternative security relationships to NATO.	Create bastion defense to offset US reliance on air & maritime platforms. Threaten to impose heavy casualties through conventional & nuclear capabilities & policies. Challenge US thinking by using overt & covert activities that inflict harm on its interests but do not validate the use of military power. Exploit US legal safe havens by using non-attributable means, commercial cut-outs, & other deniable illicit activities.
Economic (aid, trade, export controls, sanctions, rewards)	Increase capabilities & presence in Arctic for resource access & to alter trade routes. Enhance relations with China & support BRI as means to increase own economic power & balance against US.	Pursue alternatives to US dollar & global leadership. Exploit US partners' energy reliance to undermine relationships & gain favorable policies. Use ties with regional powers to deny US access.	Build & maintain strong economy & expand trade partners to undercut US faith in economic tools of power.
Information (exchanges, press releases, speeches, visits, influence in forums, trust building)	Use deception to confuse, overwhelm, & mislead decision-makers. Raise questions about the reliability & sources of information. Use public speeches in UN, etc. to communicate positions, enhance image, demonstrate resolve, & undercut US influence. Covert propaganda to undermine NATO & US cohesion while creating uncertainty.	Active measures to undermine US / NATO partners' credibility, exacerbate social & political divisions, & exert pressure. Develop cultural connections with US population to undercut support for counter-Russia policies. Espionage to undermine US / NATO operations security & confidence. Paint West as exploitive vs. Russia's support for UN principles.	Propaganda to demonstrate duplicity in US values-centric arguments, capitalist norms, & support for human rights. Challenge US self-image and ideas of exceptionalism. Exploit open society & political system.
Technology (advanced R&D, investments)	Heavy investment in security related R&D to create small, highly capable nuclear, conventional, & unconventional forces that offset US hard power advantages. Developed hypersonic missiles, high speed torpedoes, & other cutting-edge capabilities.	Espionage to offset US technology advantages & rapidly advance own capabilities. Support domestically produced cryptocurrency.	Exploit US reliance on technology through heavy investment in electronic warfare & cyber. Espionage to gain advances cheaply & counter US tech. Develop advanced systems capable of holding expensive US assets at unacceptable risk.
Geography (open ports, proximity, & relationships)	Establish military bases & relationships along maritime chokepoints & other key regions to undermine US sense of security & perceptions of own power. Use constrained geography to create bastion defense.	Propagate Greater Russia that extends beyond borders to challenge Westphalian concepts. Exploit proximity & connections to Arctic, Europe & Central Asia to counter US access & influence. Use proxies & partners to undermine US ability to deploy forces.	Use Cuba & Venezuela to exert pressure on US historical sphere of influence. Use US logistical requirements as leverage with NDN & Afghanistan operations. Expand capabilities in Arctic where US was underinvested.
Cyber activities	Become one of the most active & capable cyber actors. Create strategic dilemmas & confusion through limited attribution & information overload. Conduct sabotage or hold critical infrastructure at risk. Undermine US intelligence, decision making, & perceptions of how to measure & employ power.	Exploit internal divisions in US & partners. Sow uncertainty on source of activities. Directly target foreign populations through social media using trolls & bots to proliferate division & sow confusion. Undermine confidence in US electoral processes through influence, hack & release operations. Hacking to feed trolls, propaganda, & develop targets.	Exploit US hard power strategic culture through use of cyber capabilities to attack foundations of society, military technology, and decision-making processes. Challenge decision-making rooted in hard power, legal norms & clear attribution. Undermine open society, values, & electoral system.

International Conflict in the New Era of Conflict

As with the previous chapter on the Cold War, in this section I will use the results of the above analysis to develop a conceptual model of international conflict during the 2007 – 2018 timeframe. This process will involve three steps. First, to provide a common baseline, I will synthesize the US and Russian approaches to conflict across the elements of power. Second, using these findings, I will summarize the synthesis in a table of commonalities. This will show how the states collectively used their elements of power to impact their opponent's neoclassical realist intervening variables. Third, I use the table to develop visual models that demonstrate how the elements of power were employed. Together, these models and the associated data will serve as the foundation for conclusions on the New Era of Conflict and the final chapter's comparative analysis.

Synthesis of Ways, Means, & Ends

During this phase of the New Era of Conflict, the US and Russia pursued substantially different goals and, in many ways, employed divergent strategic methods to achieve them. This presented significant challenges to constructing a common approach to international conflict, although there was sufficient overlap in how the states applied their elements of power to enable a useful synthesis. At the same time, however, the construct glosses over some important aspects of the conflict that will be captured in the dissertation's conclusion.

From the perspective of the military element of power, both states emphasized deterrence and shaping operations directed at the other's behaviors. While Russia pursued an economy of force approach and the US continued to spend heavily on defense, the states both upgraded their nuclear capabilities and invested in advanced conventional military systems, which they deployed globally to demonstrate power, influence other states, attack other adversaries, and support their regional interests. In addition, although the US and Russia did not use force directly against each other, their proxies did engage in combat against the opposing state and its allies. Finally, both states used foreign arms sales, security organizations, and engagements to shape the international environment and build access and influence. Therefore, the military element of power was critically important to both states as they used it to build influence, enhance their international status, and undercut the other's power.

Economically, the US and Russia both used their power to coerce, cajole, and coopt other states in pursuit of their interests. Specifically, the US leveraged its position in the global monetary system, banking industry, and as the leading economy to gain cooperation and move states away from dependence on Russian petroleum resources. The US also provided aid to countries with which it wanted to gain access and influence and coerced those that acted against its interests. This included Russia, against which the US used sanctions to weaken its centralized power structure and undermine its economic and domestic security. Moreover, the US exploited its oil production to undercut Russia's primary income source. Russia too, used petroleum products as an economic tool to build relationships and coerce other states. Moreover, it developed closer relations with China and supported BRI to strengthen its economy and balance against the US. Finally, Russia worked with other states to develop parallel international organizations and strengthen alternative currencies as ways to weaken the United States' economic weapon and to protect itself against coercion. Thus, collectively, the US and Russia used their economic power for positive and negative purposes, focused on strengthening their position and weakening their opponent's, particularly in the petroleum industry and trade relationships.

Technologically, both states made substantial investments in security-related research and development to enable other elements of power and advance their interests. For the US, this was a critical component of its Third Offset Strategy and a foundational element of its economic power. In addition, the US sought to undercut Russian security through technological advancements such as missile defense, artificial intelligence, and space capabilities, while it also imposed restrictions on technology exports to Russia. Finally, the US used its leadership in ICTs to maintain an open internet despite Russian attempts to gain sovereign control over the domain.

While Russia pursued a similar path, it applied technology with more precision, pursuing a small, highly capable, cutting edge military that led in specific areas such as hypersonics, cyber capabilities, and electronic warfare. For both states, therefore, technology was a critical enabler for their other elements of power and an important part of their international image.

From an information perspective, the US used international bodies, statements, and press to expose Russian malfeasance, offset its propaganda, influence allies, and communicate resolve to opponent leaders. It also attempted to use information to undermine Russian domestic security, confidence, and centralized control, while propagating its values on human rights and free trade. For Russia, information was its most important element of power, which it used for both defensive and offensive purposes. Specifically, Russia sought to counter US efforts to propagate its values, which it perceived as a threat to international and domestic stability. At the same time, however, Russia also used information to create confusion, overwhelm decision-makers, and undercut US influence by exposing its perceived hypocrisy. In the process, Russia attempted to divide NATO, undermine the idea of US exceptionalism, and attack US domestic stability through propaganda campaigns and hack and release operations. Espionage also to an important role for both powers, as the information it provided allowed them to understand and counter their opponent's plans and operations across all elements of power. Thus, the US and Russia used information power to attack their adversary's domestic security and international influence while they also employed it to support other activities.

Geography was important to both states, as each used its location and access to support other instruments of power and gain advantages in strategic regions. In addition, Russia and the US used their global capabilities to undermine the other's sense of security, enhance their international image, and develop relationships with key states. Collectively, these efforts provided the states with strategic leverage, influence, access, and critical resources.

The states' exploitation of cyber technology had a broad impact across all elements of power as it served as an enabling platform while also creating vulnerabilities that had to be addressed. As a result, the US and Russia took both offensive and defensive actions in cyberspace as they sought to become leaders in the domain and used it to further their grand strategies. Specifically, both states used the domain as a battlespace, income generating platform, research and development capability, venue for proliferating ideas and information, and a mechanism for espionage and sabotage. These activities were greatly enabled by the technology's ubiquity and limited attributability, which allowed the US and Russia to gain increased access to their opponent's populations and critical infrastructure, while also allowing them to create global effects, even in places where they had limited presence. Thus, as summarized in Table 6, for both states, cyber technology provided extensive opportunities to gain accesses and create effects that magnified their elements of power and supported their grand strategies.

Table 7: International Conflict in the NEC

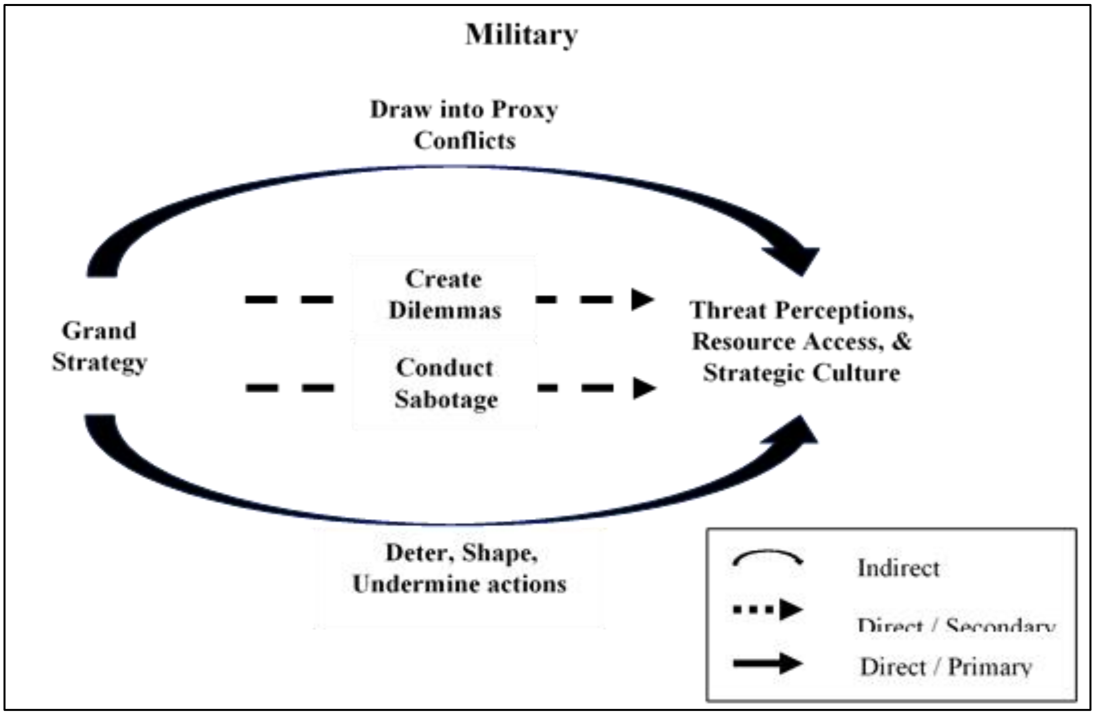
Variables Elements	FPE Perceptions	Ability to access & employ resources	Strategic Culture
Military (nuclear & conventional forces, security assistance)	Modernize nuclear triad & develop or maintain strong conventional military to deter adversary. Use force to protect interests. Use proxies to directly compete with opponent in key areas. Use overt & covert military to expand power, & complicate adversary decision making.	Employ proxy forces to undermine adversary access to strategic areas. Use arms sales to gain access & influence in key countries. Create strategic dilemmas for opponent alliances & force employment. Leverage security -related institutions to create collective strength & build relationships.	Challenge opponent's thinking, decision making, & risk calculus through overt & covert activities that inflict harm on its interests. Create strategic dilemmas.
Economic (aid, trade, export controls, sanctions, rewards)	Enhance trade relations with other countries to increase relative economic power. Undermine opponent's opportunities & sense of economic security.	Manipulate oil resources to impact opponent's economy. Use aid to build relationships and offset opponent's influence in key countries.	Use economic tools to avoid military strengths & impact risk calculus.
Information (exchanges, press releases, speeches, visits, influence in forums, trust building)	Use public speeches & press statements to communicate positions, enhance image, demonstrate resolve, & undercut other's soft power.	Communicate with adversary's people to undermine domestic control & interfere with governance. Expose opponent's secrets & apparent malfeasance to weaken its partnerships & popular support. Use espionage to reduce effectiveness of adversary's plans & operations.	Challenge opponent's self-image and ideas of exceptionalism.
Technology (advanced R&D, investments)	Heavy investment in security related R&D to create highly capable forces that deter opponent. Undercut each other's security through technological advancements.	Develop capabilities to deny adversary flexibility & employment of own resources across all domains and elements of power.	Exploit adversary's reliance on technology through investment in countermeasures or superior capabilities. Develop advanced systems able to hold other's assets at unacceptable risk.
Geography (open ports, proximity, & relationships)	Demonstrate global reach & establish military bases & relationships to undermine opponent's sense of security & challenge perceptions of power.	Exploit proximity & connections to important regions & chokepoints to counter opponent's access & influence. Through key relationships, undermine adversary's ability to deploy forces & access critical resources.	Use geographical position & develop relationships to exert pressure on historical spheres of influence.
Cyber activities	Develop & employ advanced cyber capabilities that enable other elements of power & challenge adversary's metrics. Use cyber activities to avoid strengths & exploit weaknesses. Create confusion by overwhelming decision-makers with vast amounts of questionable data.	Access adversary populations to undermine support for government. Rapidly & broadly disseminate information to challenge adversary's power. Conduct cyber sabotage or hold critical infrastructure & data at risk. Sow uncertainty on source of activities to hinder countermeasures.	Create strategic dilemmas for decision-making processes, challenge structures, & exploit rigid cultural norms that undergird leadership confidence in decisions & information sources.

Conflict Models

To provide a common comparative framework between the case studies, in this section I will apply my research framework to the above analysis to generate visual models of international conflict for the respective time periods. In the process, I will develop a total of six models, with the first five examining how each element was used to create effects on the adversary's intervening variables.[4] In addition, to evaluate my independent variable, I will provide a model for cyber technology. Taken together, these models and their supporting analysis will support my ultimate analysis on the character of the New Era of Conflict.

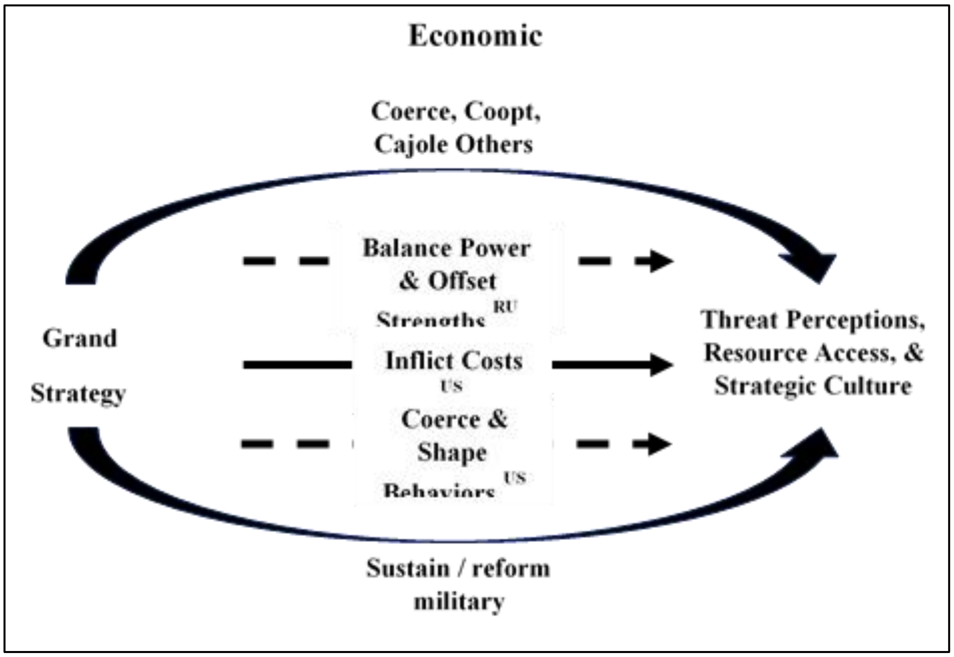
As reflected in Diagrams 8 through 13, the elements of power that played the heaviest role in the New Era of Conflict were information and economic power, with the former being Russia's primary tool and the latter the United States'. Thus, while the military element was important, it was mainly used in an indirect manner, as was geography, which played a largely supporting role, enhancing other elements of power and providing advantages to be exploited. Technology, however, grew in importance, as a capability for Russia to directly offset some of the United States' strengths, the cradle of the cyber domain, and the backbone of economic power.

[4] Direct includes the use of an element to produce an immediate effect without an intervening party or other influence. Indirect, however, is the use by or through a third party or in a way that does not employ the capability to its full, traditional extent. For example, direct use of the military would be a kinetic strike, while indirect use would be using it to deter an opponent.


Military
Draw into Proxy Conflicts
Grand Strategy
Create Dilemmas
Conduct Sabotage
Threat Perceptions, Resource Access, & Strategic Culture
Deter, Shape, Undermine actions
Indirect
Direct / Secondary
Direct / Primary

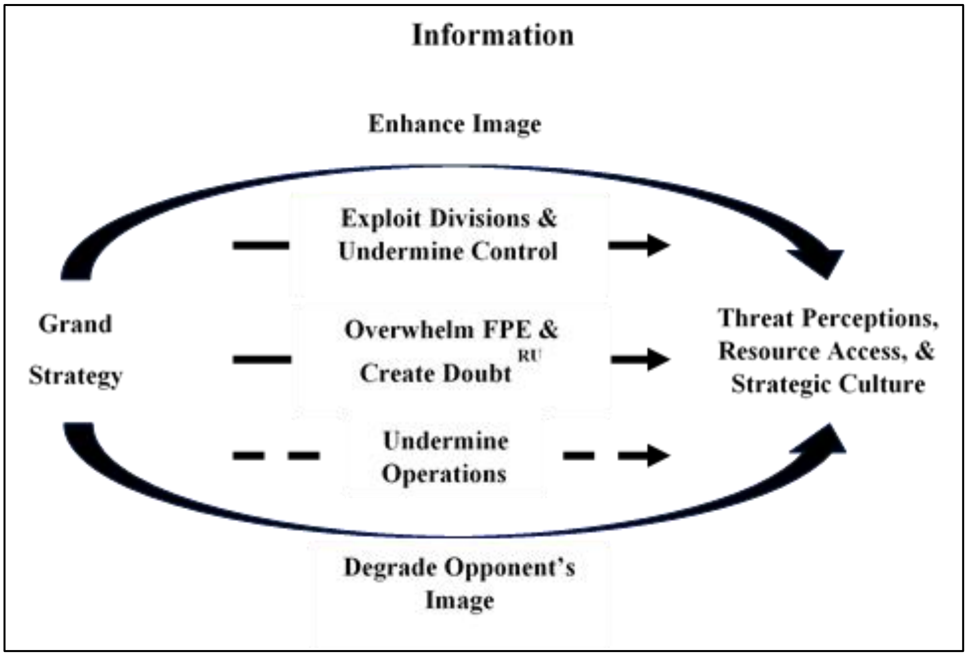
Military Conflict in the New Era of Conflict

Diagram 8


Economic
Coerce, Coopt, Cajole Others
Grand Strategy
Balance Power & Offset Strengths RU
Inflict Costs US
Coerce & Shape Behaviors US
Threat Perceptions, Resource Access, & Strategic Culture
Sustain / reform military

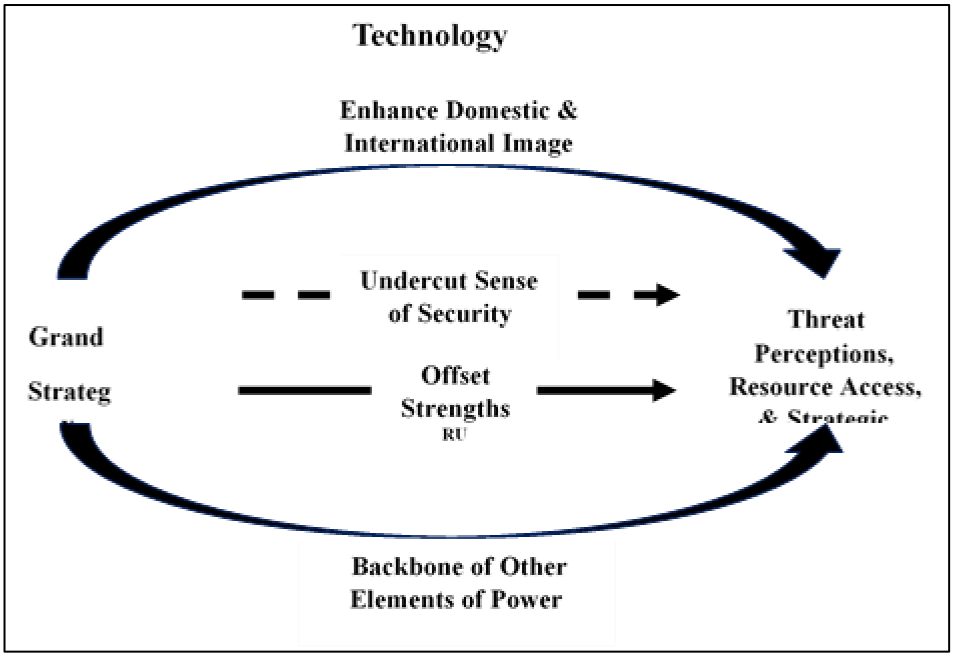
Economic Conflict in the New Era of Conflict

Diagram 9


Information
Enhance Image
Exploit Divisions & Undermine Control
Grand Strategy
Overwhelm FPE & Create Doubt
RU
Threat Perceptions, Resource Access, & Strategic Culture
Undermine Operations
Degrade Opponent's Image

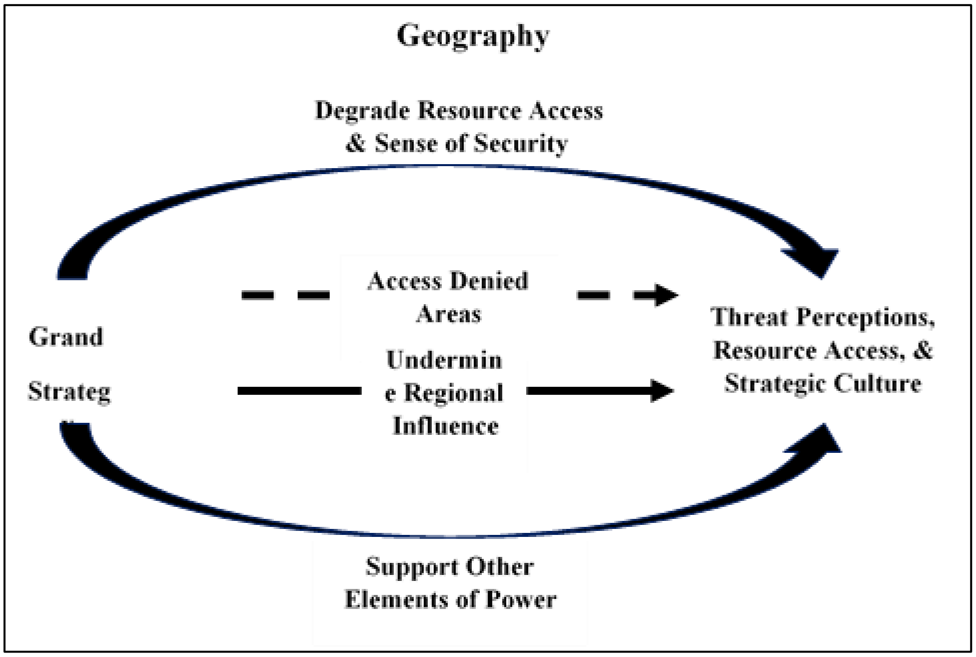
Information Conflict in the New Era of Conflict

Diagram 10


Technology
Enhance Domestic & International Image
Undercut Sense of Security
Grand
Strateg
Offset Strengths
RU
Threat Perceptions, Resource Access, & Strategic
Backbone of Other Elements of Power

Technology Conflict in the New Era of Conflict

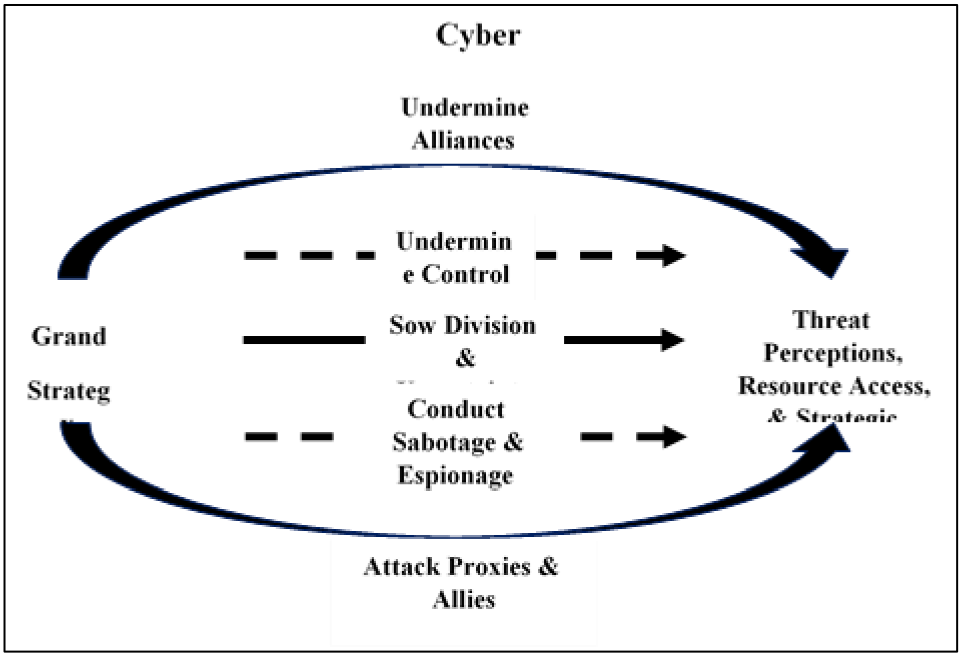
Diagram 11



Geography Conflict in the New Era of Conflict

Diagram 12

Finally, and most importantly for the purposes of this research, is the role cyber technology played in the conflict. As represented in Diagram 13, Russia and the US used cyber technology to directly impact the other's internal control, societal unity, and decision-making processes. In addition, the states used it to conduct sabotage operations, access denied areas, and as a venue for unparalleled access to sensitive information. Due to its ubiquity and robust architecture in both states, cyber technology also enhanced information power by allowing the actors to greatly increase the scope and reach of their activities. Thus, cyber technology fulfilled a fundamental supporting role for all the elements of power, in the process enabling the states to take direct actions against their adversary where other traditional capabilities would have posed an unacceptable risk of detection or excessive costs.



Cyber Conflict in the New Era of Conflict

Diagram 13

Conclusion

Since 2007 the United States and Russia have been engaged in an increasingly contentious conflict that has cost billions of dollars and an untold number of lives. While this conflict has not dominated the international system to the same degree as the Cold War, it has nonetheless created effects across the globe, as the states have engaged in proxy battles, nuclear threats, confrontations at sea, and extensive campaigns against each other in the media and cyber spheres. Thus, despite its more limited scale, the conflict has been an enduring global struggle with high stakes and real costs.

To understand this New Era of Conflict and provide a foundation for comparison with the Cold War, in this chapter I analyzed its development over the 2007 – 2018 timeframe. This period was selected since it involved a similar duration as my first case study. In addition, the time period included the conflict’s initial days, which I argue were marked by Russia’s extensive cyberattacks and propaganda campaign against Estonia in April and May of 2007.

To conduct this case study, I followed a four-step process that mirrored the approach in the previous chapter. Specifically, I first examined the roots of the conflict and developments in the international system that led up to the timeframe under study. This step allowed me to establish the historical foundations for the subsequent analysis and also to gain an understanding of the conflict’s causes and enduring challenges.

Second, I conducted a detailed analysis of the grand strategies each state followed during the time period. Before delving into the specifics, however, I first examined government documents and scholarly assessments to determine whether the US and Russia followed consistent grand strategies throughout. Although I concluded that each state did pursue enduring strategic objectives, I also found that the ways they applied their elements of national power evolved over time due to domestic and international developments. With that established, I then evaluated the grand strategies from a ends, ways, means perspective, in the process analyzing how each state applied their elements of power to achieve their strategic objectives. As part of this, I also highlighted the role cyber technology played by specifically calling out how the US and Russia used it in the course of the conflict.

Third, to understand the potential impacts of the US and Russian grand strategies, I evaluated the ways each state used its elements of power and cyber technology to target the opposing state’s neoclassical realist intervening variables. Through this process, I was able to highlight the states' attempts to attack these vulnerabilities through various means and methods, thereby capturing the character of conflict over the decade.

Finally, I synthesized these findings and used the results to develop models that reflect how the states collectively employed and prioritized each element of power and cyber technology. While this step was largely successful, it is important to note that there were significant variations in the US and Russian approaches, which resulted in more complex models than were developed on the Cold War. Thus, while there was significant overlap in US and Russian strategies relating to some elements of power, they diverged sharply on others. This was particularly true of how they prioritized information and economic power, which Russia and the US more heavily favored, respectively.

While these differences are important to keep in mind, and will be further examined in the next chapter, the above analysis nonetheless discovered important characteristics about the New Era of Conflict overall. Specifically, based on the states' behaviors, it is evident that the meaning of power is being challenged as the US and Russia have sought to employ both traditional and novel means to offset the other's advantages and exploit its weaknesses. Moreover, and of greatest importance for this study, is the finding that cyber capabilities undergirded many of these efforts.

Taken together, the above analysis and its findings raise fundamental questions about the New Era of Conflict and my hypothesis. How, for instance, do its characteristics differ from the Cold War? Why has conflict changed or stayed the same? And, what role did cyber technology play in the process? These questions will be the focus of the next chapter as I conduct a comparative analysis of the two cases and ultimately test my hypothesis on the impact of cyber technology on international conflict.

Chapter Six: Assessing the Hypothesis

Introduction

This project is about international conflict, one of the most studied topics in political science. Throughout recorded history, scholars and practitioners have engaged in extensive research and analyses to gain a greater understanding of how to prevent, win, and end conflicts. Despite the myriad of articles and books about the topic, however, conflict remains a controversial enigma that, while perhaps mitigated, has yet to be controlled.

Although many factors have influenced the course of conflict over the millennia, technology has played a central role in how it has evolved. From the longbow to the stealth fighter, technological developments have given states the edge in combat or provided advantages as deterrents or coercive tools. Technology's impact, however, has also reached beyond weapons, to influence every element of national power and, thus, international relations writ large. As has been demonstrated repeatedly throughout history, the side that employs technology most adeptly often achieves a decisive advantage.

In the Twenty-First Century, one of the most ubiquitous and revolutionary developments has been cyber technology. From its humble beginnings in a controlled lab environment to its deep integration into nearly every aspect of our daily lives, cyber technology has become a critical resource for states and societies. In the process, it has had both positive and negative effects, as people have used it for good and for ill. This is no less true of states, which have sought to employ cyber technology to improve governance and to gain advantages in the struggle for international power.

Despite its ubiquity, however, there is much yet to learn about cyber technology and international conflict. While scholars have engaged in numerous studies on their relationships, the analyses have reached broadly disparate conclusions. As such, there is a substantial lacuna in the literature relating to cyber technology. This project sought seeks to address this gap in part by examining how cyber technology is impacting international conflict. In the process, it takes a uniquely holistic approach to the technology while also adopting a broad definition for conflict. Thus, rather than focusing on discreet effects or warfare, this study looks at cyber technology's potential effects in their entirety and treats international conflict not solely as an armed exchange but the broader competition for power between states.

To provide the evidentiary foundation for this effort, in the two previous chapters, I conducted a detailed examination of the grand strategies the US and Russia adopted during the Cold War (1980s) and New Era of Conflict (2007-2018). As part of these analyses, I developed matrices and models that demonstrate how the states used their elements of power to exploit their opponent's decision-making vulnerabilities. Moreover, to provide data on cyber technology, in the first substantive chapter, I conducted an extensive study of its history and how it has become so heavily integrated into modern society. In the process, I created a framework of cyber-related vulnerabilities and highlighted their potential impacts on how states form and implement their grand strategies.

In this chapter, I will use the above data to conduct a comparative analysis of the case studies, examine the findings, and assess my hypothesis that cyber technology is having a novel and fundamental impact on international conflict. This will involve three steps. First, I will compare the evidence drawn from the two case studies to identify similarities and differences in how the states employed their elements of power during the two conflicts. Second, I will use the evidence contained in the previous chapters to analyze the association between the changes that occurred over time and the revolution in cyber technology. As part of this process, I will address the study's research questions and evaluate my hypothesis. Finally, I will identify gaps, highlight further research areas, and discuss the policy implications of my findings.

Collectively, this analysis will demonstrate that international conflict has changed significantly over the past forty years due to multiple, interrelated variables. While cyber technology alone was not responsible for all of these developments, it nonetheless provided states a domain through which to gain unprecedented access to and influence on its opponent's neoclassical realist intervening variables. As such, cyber technology has played a significant role in the changes we have seen and, in view of its increasingly important role in a functioning society and government, will likely continue to shape international conflict well into the future.

Case Study Comparison

As discussed in the two previous chapters, during each of the periods of study the US and Russia followed enduring grand strategies that remained largely consistent, although they evolved with domestic and international conditions. By analyzing these grand strategies from a ends, ways, means perspective, I gathered a substantial amount of data and constructed matrices and models that collectively provide the foundation for a comparison of the two eras of conflict.

Before delving into the comparative analysis, however, I will first outline the data and conclusions from each of the case studies. In the process, I will focus on how the states employed their elements of power, directly and indirectly, to impact their opponent's neoclassical realist intervening variables. With this foundation set, I will then compare the cases and develop a table of similarities and differences. This will set the stage for my analysis of cyber technology's impacts in the second step.

The Cold War

During the 1980s, one of the major factors influencing conflict between the United States and Soviet Union was their massive nuclear arsenals, which not only deterred the other state but also limited the use of military power to a largely indirect role. As a result, the militaries did not conduct kinetic operations against the other's forces but were mainly used to create strategic dilemmas and play on the opponent's fears. To achieve these goals, the US and USSR deployed air, maritime, and land assets near each other's borders and other sensitive areas, showcased their military capabilities, used weapons and other resources to support or recruit partners, and engaged in non-violent confrontations. Where armed conflict did ensue, it invariably involved proxy forces, which provided a level of deniability or limited accountability for the resulting deaths and destruction.

Unlike the military, however, economic power played an important direct role in the conflict. Specifically, both the US and USSR used inducements and penalties to encourage the other to cooperate or stop engaging in behaviors they believed to be harmful to their interests. In addition, the states used economic power indirectly to support their ideology, expand their influence, and build capabilities for themselves and their allies and proxies. Thus, the US and Soviet Union used sanctions, aid, arms sales, and economic performance data to support their strategies while undermining the other's directly and indirectly. As the decade wore on, however, and the economic disparity between the states widened, this element grew in importance, with the US leveraging its advantage to exert increasing pressure on the Soviet Union's FPE and flagging finances.

Similarly, information played direct and indirect roles, as the states sought to build their own brand and counter their opponent's by undercutting their soft power, exacerbating domestic divisions, and harming international relationships. As part of this effort, the US and USSR used information to create or exploit domestic divisions, raise questions about the other government's efficacy, and undermine FPE perceptions of security. In the process, they used overt and covert media posts, radio broadcasts, public statements, infiltration into domestic organizations, and aggressive espionage and counterintelligence programs to directly and indirectly attack the other's intervening variables in ways that were not feasible with the other elements of power. For the Soviet Union, this was a particularly valuable resource, as it was inexpensive and greatly facilitated by the United States' open society.

The states also used technology directly and indirectly, although it mostly played a supporting role to the other elements of power. Specifically, for the US and USSR, technology provided a means for increasing their military capabilities, building economic power, supporting ideological arguments, enhancing their international image, and influencing potential partners. In addition, the states used technological advancements to reduce unfavorable power disparities and improve on others, while simultaneously working to undermine their opponent's. Since the US offset strategy was based on qualitative superiority, advancing and protecting its technological edge was critically important. As such, technology was an area of persistent struggle between the states and a priority for Soviet espionage activities.

Finally, the US and USSR both leveraged their geographic positions and global reach to directly interfere in the other's perceived spheres of influence and threaten their access to critical resources. Moreover, the US and USSR exploited the other's geographical disadvantages, such as the Soviet's constrained maritime access, the United States' open coastlines, and Europe's proximity and vulnerability to land invasion, as opportunities to collect intelligence, constrain their opponent's activities, undermine their sense of security, and create the perceived need to invest resources in protective countermeasures. In addition, the states used their global capabilities to indirectly exploit critical lines of communication and negatively affect FPE perspectives through deployments and intelligence collection operations near their homelands.

Collectively then, conflict in the 1980s was primarily focused in the information, economic, and military realms, with the first playing a larger part in the struggle than is typically acknowledged. Although geography and technology also were critical in certain respects, they mainly filled supporting roles. That said, it is important to note that the states prioritized their elements of power differently, with the US and Soviet Union relying more heavily on economic and information power, respectively.

The New Era of Conflict (NEC)

Like the Cold War, during the NEC, nuclear weapons played a key role in constraining the direct use of military power against the opposing state. As a result, the US and Russia mainly employed their militaries indirectly, as deterrents and to gain access and influence in regions that offered a potential advantage. In addition, Russia and the US used their militaries to create strategic dilemmas for each other, by placing forces in disconcerting locations, invading or attacking the other's partners, and employing proxies against their forces and interests. At the same time, however, the US and Russia took a novel step by using cyber technology to conduct attacks against the other's forces and homelands, particularly as a mechanism for gaining access to information and in preparation for sabotage against their critical infrastructures.

Economically, both states looked for opportunities to gain relative power, although there was a significant mismatch between the two. Due to its substantial advantage in this realm, the United States relied heavily on inducements and coercive measures, with the latter becoming more widely used as the decade wore on. Since Russia was in an economically weaker position, however, it sought to undermine the US and offset its advantages by creating alternative economic mechanisms and currencies, developing the Arctic trade route, and cooperating with China. In addition, Russia achieved some significant economic improvements over the decade, and it leveraged its oil resources as a tool to create dependencies, enhance relationships, and coerce other states. Moreover, while both powers engaged in arms sales to cultivate relationships and gain access and influence with strategically important states, Russia also used them to create divisiveness between the US and its allies.

Information once again played an important role as a mechanism for the states to enhance their own image and create challenges for their opponent. Specifically, the US and Russia used information to undermine the other FPE's sense of control, create or exacerbate internal divisions, hinder international relationships, and raise questions about the reliability of the data they were receiving. Although both states used traditional methods, such as radio and television broadcasts to disseminate their narratives, the US and Russia also relied heavily on cyber technology, which proved a critical resource for rapidly distributing large amounts of information to target audiences around the world, including their adversary's populations.

This approach was especially important to Russia, which exploited the openness of US society and the internet's architecture to bombard its opponent with vast amounts of information designed to exacerbate social and political tensions, exploit biases, and overwhelm decision-makers with questionable data. Additionally, while both states engaged in extensive cyber-based espionage, Russia was particularly aggressive in exploiting the capability to not only gain access to sensitive military data but also to engage in hack and release operations through which it obtained and selectively exposed secrets and divisive information.

Technology once again played a critical supporting role as the US and Russia sought to exploit advances to enhance their military, economic, and information power. In the process, both states used technology to improve their domestic and international image, support relationships with other states, and undermine their adversary's sense of security. These drivers were particularly true of missile defense, space-based platforms, artificial intelligence, and hypersonic missiles, which offered significant advantages by undercutting their opponent's power, reducing their flexibility, and challenging their strategic calculus. Advances in cyber technology were also crucial, as the domain became increasingly important to each state's national security and society, and thus developed into a growing battlespace with international and domestic impacts. While the US was largely seen as the leader in many areas of technology, Russia nonetheless greatly enhanced its power over the course of the decade, especially in its work on missile systems and cyber capabilities, which it used to undermine its opponent's strengths.

Geographically, the US and Russia sought to create and exploit advantages by imposing on the adversary's spheres of influence, dominating critical lines of communication, offsetting their opponent’s access and influence, and placing the other’s homelands and resources at risk. To accomplish this, the states built relationships with strategically positioned partners, deployed forces to sensitive areas, and improved their abilities to create effects anywhere on the globe. In addition, Russia worked to enhance its security and influence by exploiting enduring cultural and historic relationships with geographically proximate states and improving its capabilities and presence in the Arctic. For the US and Russia, cyber technology provided both opportunities and risks, as it allowed them to mitigate some geographic constraints such as distance, terrain, and international borders when employing their other elements of power.

Taken together, the above demonstrates that The New Era of Conflict was dominated by military, economic, and information power, with technology and geography serving in largely supporting roles, although the former grew in importance. Information once against proved to be a critical capability for both powers, with cyber technology greatly enhancing its scope, precision, and reach. In addition, the US and Russia prioritized their elements differently, with the former emphasizing its economic power and the latter information.

Conflict Comparison

To understand the differences between the two conflicts and some of the driving forces behind them, in this section I will conduct a comparison of the two periods across the states’ elements of power. In the process I will also highlight some important environmental factors that influenced the course of events. While this step is not intended to identify all the potential variables and thus rule out multiple causal processes, it nonetheless will provide important context for how and why conflict evolved.

From a military perspective, the Cold War and New Era of Conflict were similar in that nuclear deterrence played a significant role in the states' strategic calculi. Although both powers' arsenals were significantly reduced before the NEC, the US and Russia nonetheless invested in their nuclear triads and updated their doctrines to address perceived threats. Moreover, in both conflicts, the states used their militaries to expand their influence, protect their homelands, create strategic dilemmas, and send messages through the deployment of forces to sensitive areas. Finally, they used proxy forces to impose costs on the other and weapons sales to gain influence and access with strategically important partners.

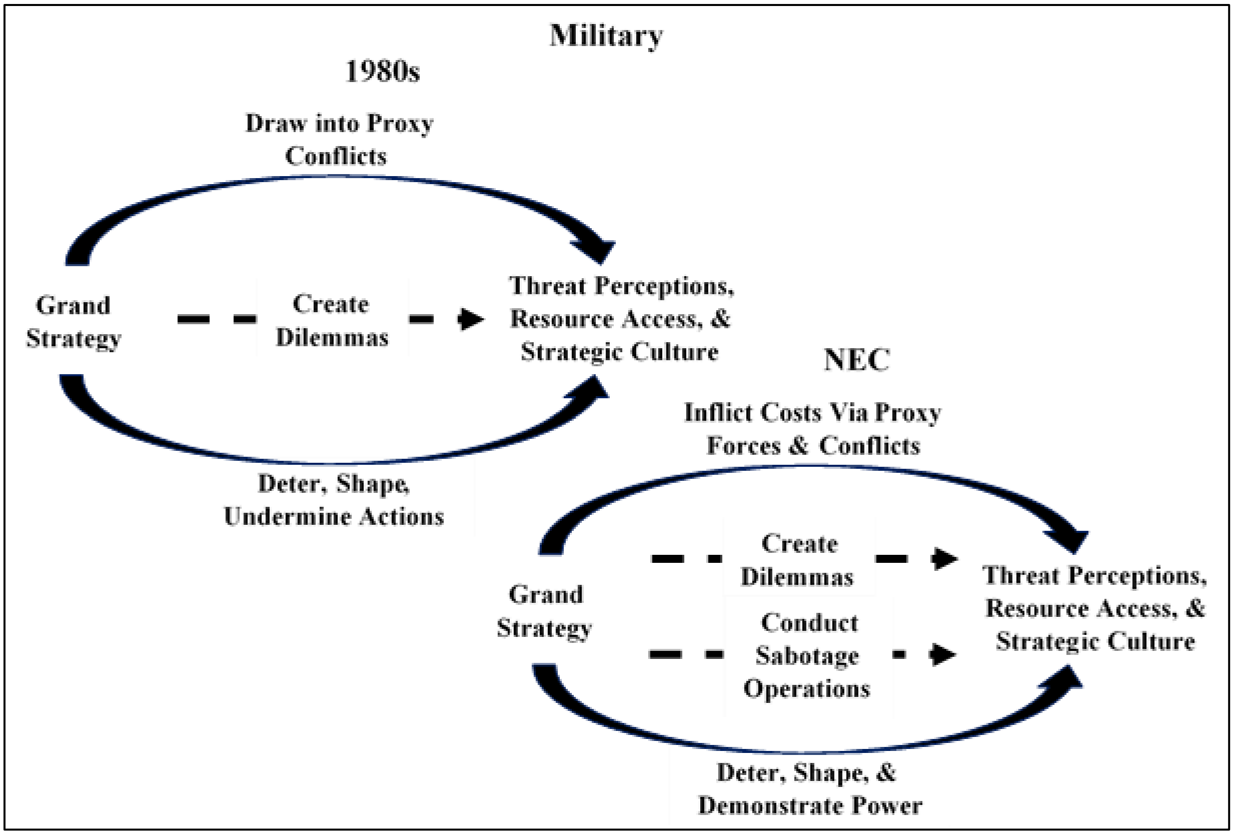
However, there are two important differences in how the US and Russia employed their military element during the periods. First, while the Cold War had a significant numerical component to how power was measured, the New Era of Conflict focused on qualitative metrics. This was mainly a change for Russia which, driven by its weaker position and lessons from the Georgia invasion, made wholesale modifications to its doctrine and way of war. In the process, Russia shifted from a primarily quantitative approach to one focused on fielding a small, professional, and technologically enabled military capable of rapid covert and overt operations throughout its perceived spheres of influence.

For the United States, which had followed a qualitative superiority model throughout the 1980s, its main metric did not change. As a result, it continued to invest heavily in defense, due to its widely defined interests, generally strong economy, and perception of growing threats. Thus, while the US reduced the size of its military and updated its doctrine, it still maintained a massive force structure that was fundamentally unchanged from the Cold War.

Second, although the US and Russia avoided direct destructive attacks on each other during the1980s, in the New Era of Conflict that calculus changed. Specifically, where destructive exchanges did occur in the Cold War, they inherently involved proxy forces and were not directed against the other's homeland. This pattern remained largely true in the New Era of Conflict, except in cyberspace, where the US and Russia conducted sabotage operations against their opponent's networks and capabilities, including inside their state borders. While these operations used clandestine approaches and non-state cut outs to limit attribution, the evidence nonetheless demonstrates that Russia and the United States used cyber technology to directly attack the other on multiple occasions during the New Era of Conflict (Greenberg 2019; Sanger 2018; US Department of Homeland Security 2018). This change is apparent in a side by side comparison of the conflict models in Diagram 14.

Economically, the two conflicts share significant similarities, as in both cases the states used their power to support their militaries, build relationships, and coerce others. Moreover, throughout the 1980s and the New Era of Conflict, the US enjoyed a larger and stronger economy. Together with its leading position in the international finance system, the US used this power to cajole, coopt, and coerce other states, particularly Russia.

The conflicts diverge, however, in two important ways. First, during the 1980s, the Reagan administration attempted to impose heavy costs through limited sanctions and military expenditures that drove unsustainable Soviet investments. During the NEC, however, the US administrations took a more direct approach, in which they increasingly relied on sanctions to change Russian behaviors.

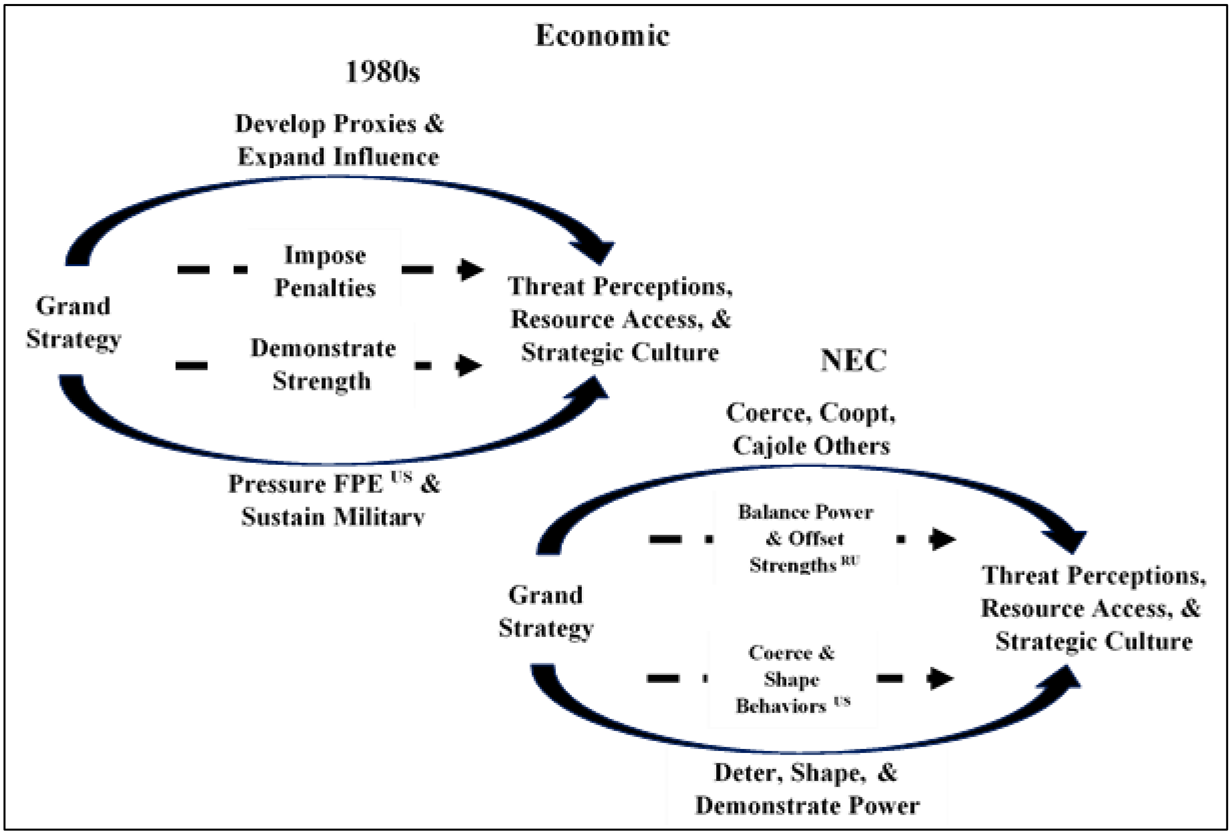

Military
1980s
Draw into Proxy Conflicts
Grand Strategy
Create Dilemmas
Threat Perceptions, Resource Access, & Strategic Culture
Deter, Shape, Undermine Actions
NEC
Inflict Costs Via Proxy Forces & Conflicts
Grand Strategy
Create Dilemmas
Conduct Sabotage Operations
Threat Perceptions, Resource Access, & Strategic Culture
Deter, Shape, & Demonstrate Power

Comparison of Military Conflict Models

Diagram 14

Second, Russia's economic situation was significantly different. Specifically, during the 1980s, the Soviet Union lost power as its economic model broke down under the weight of its own inefficiencies and pressures from its vast military budget. In the New Era of Conflict, however, Russia adopted reforms that balanced expenditures and allowed it to stabilize its economy, even in the face of increasing US sanctions. Moreover, rather than pursuing an ideologically closed economy, Russia expanded its partnerships and sought out other states, such as China, to balance against the US and create alternative currencies and financial mechanisms. Therefore, rather than attempting to demonstrate its ideological superiority and directly compete with the US through unsustainable military investments, Russia worked to offset the United

States' coercive measures and undermine its economic dominance through relationships and avoidance measures. Diagram 15 reflects these changes.


Economic
1980s
Develop Proxies & Expand Influence
Impose Penalties
Grand Strategy
Demonstrate Strength
Threat Perceptions, Resource Access, & Strategic Culture
Pressure FPE US & Sustain Military
NEC
Coerce, Coopt, Cajole Others
Balance Power & Offset Strengths RU
Grand Strategy
Coerce & Shape Behaviors US
Threat Perceptions, Resource Access, & Strategic Culture
Deter, Shape, & Demonstrate Power

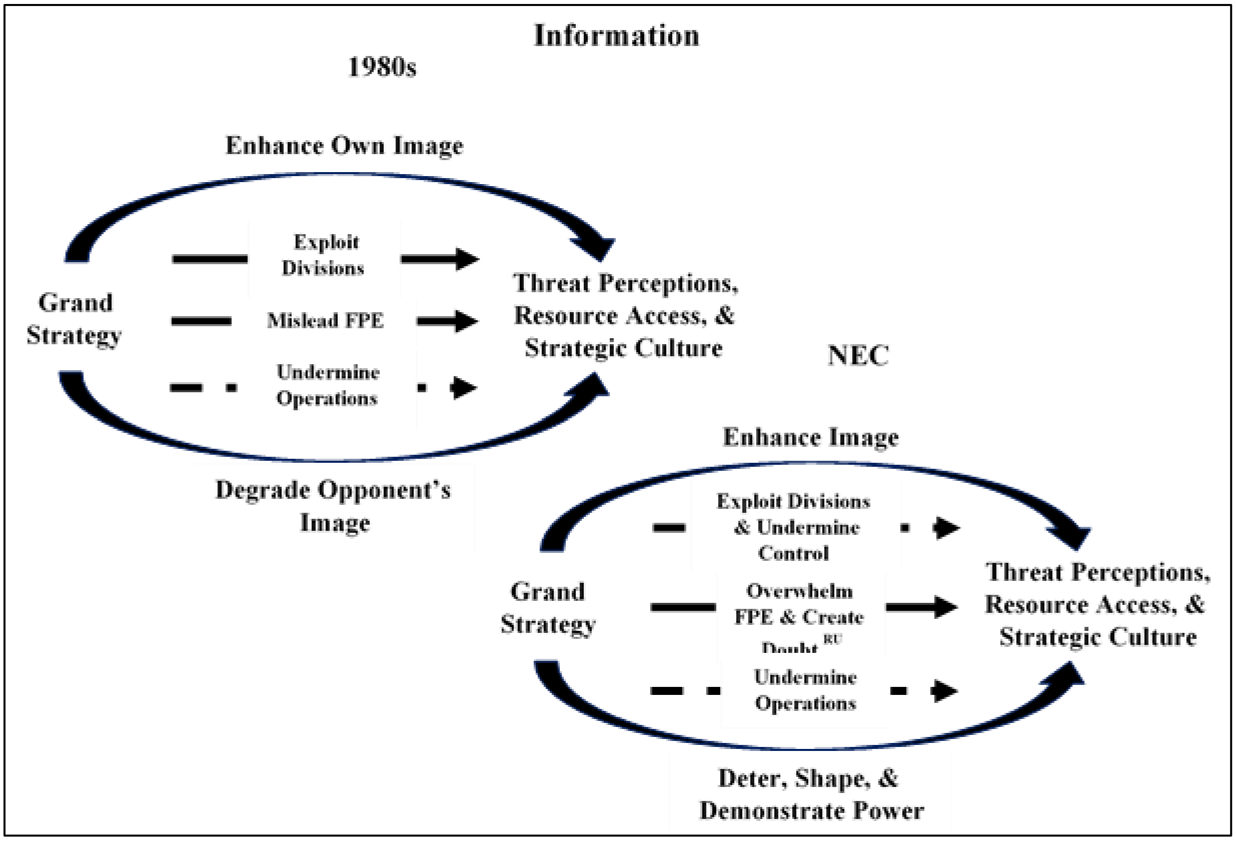
Comparison of Economic Conflict Models

Diagram 15

Regarding information, the US and Russia used it extensively during both conflicts, as they attempted to increase their international influence while harming the other's. In addition, both states sought to obtain sensitive information, undermine the other's domestic support, and create uncertainty for their FPEs. This was particularly true for Russia, as it used information power as a its primary capability to offset US advantages in other elements of power.

Although information was used in similar ways in both conflicts, the dissemination techniques and scope of application were substantially different. Specifically, during the Cold War, the United States and Soviet Union relied heavily upon the traditional press, government funded radio broadcasts, and domestic infiltrators to deliver their messages. In addition, the states engaged in aggressive espionage programs using multiple electronic and human-based collection platforms. These programs often involved third parties, long lead times, uncertain distribution paths, and specially trained operatives taking great personal risks.

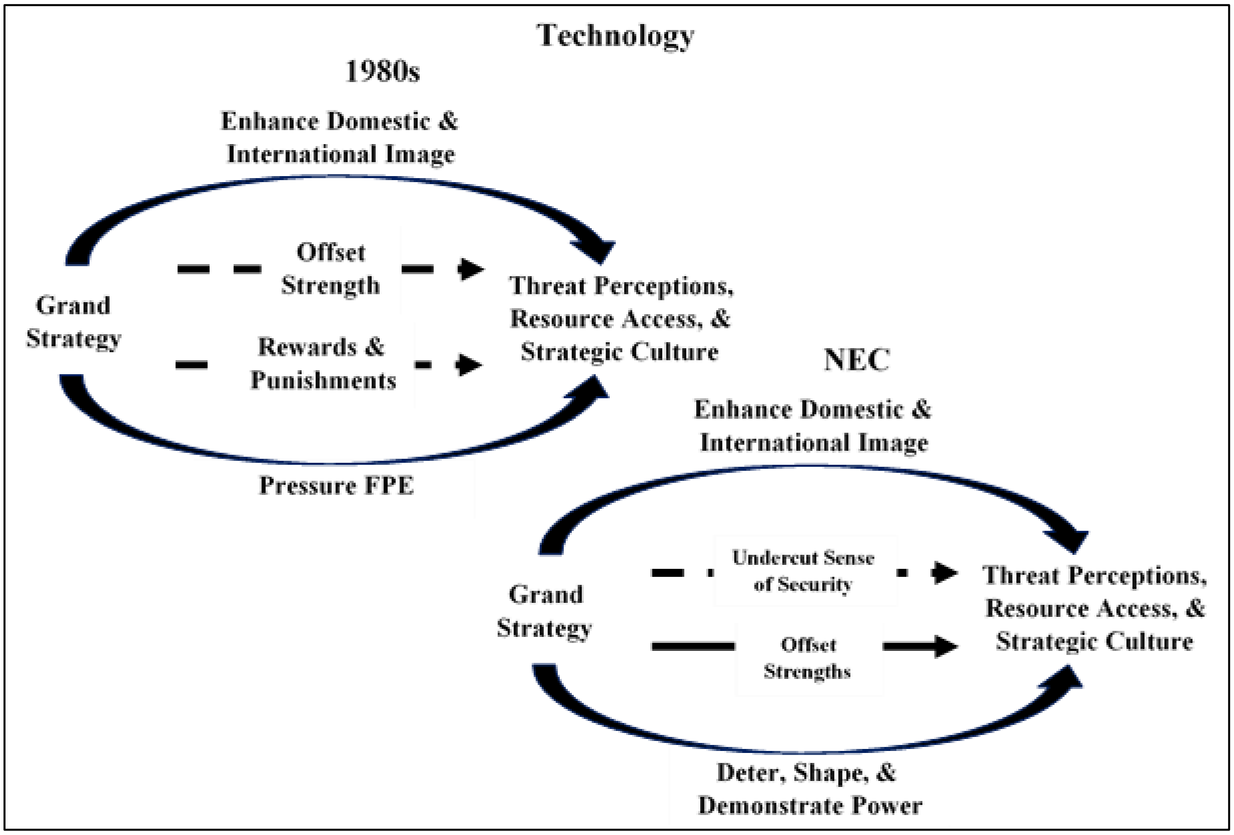
During the New Era of Conflict, however, the states actively exploited cyber technology to disseminate vast amounts of highly impactful information broadly and rapidly across international borders, directly to mass audiences or selected targets. This was especially true for Russia, which adroitly exploited social media platform algorithms, people's inherent biases, limited attribution, and the United States' open society to exacerbate social, economic, and political divisions. In addition, Russia worked to overwhelm US decision-makers through the direct dissemination of large amounts of deceptive, tailored, and inflammatory data, and it conducted aggressive cyber-based espionage and hack and release operations. Although both states also continued to rely on many of the traditional approaches employed during the Cold War, cyber technology provided them with an avenue for greatly expanded access to sensitive areas and powerful tools with which to affect vulnerable populations at much lower risk. Diagram 16 reflects these similarities and differences.


Information
1980s
Enhance Own Image
Exploit Divisions
Grand Strategy
Mislead FPE
Undermine Operations
Threat Perceptions, Resource Access, & Strategic Culture
Degrade Opponent's Image
NEC
Enhance Image
Exploit Divisions & Undermine Control
Grand Strategy
Overwhelm FPE & Create Doubt RU
Undermine Operations
Threat Perceptions, Resource Access, & Strategic Culture
Deter, Shape, & Demonstrate Power

Comparison of Information Conflict Models

Diagram 16

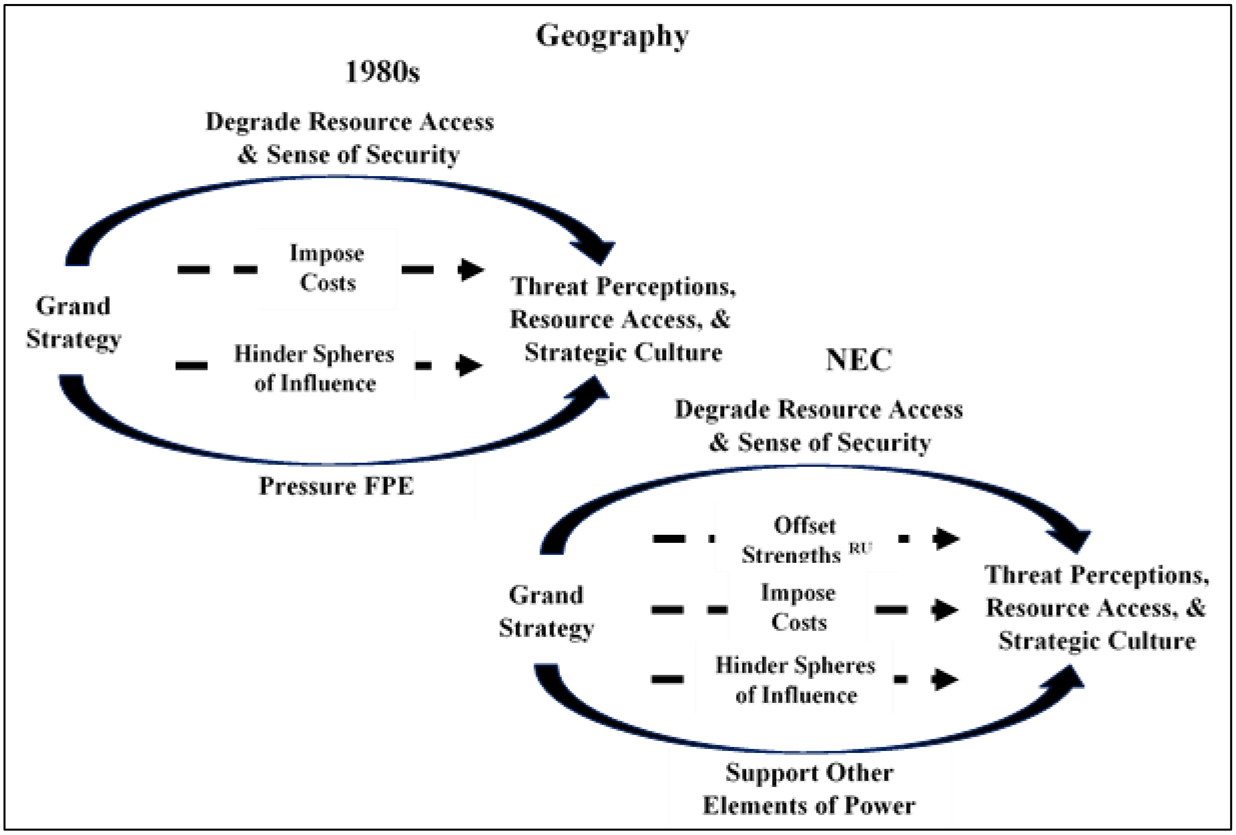
Technology played an important role in both conflicts, with the states consistently using it to pursue economic, military, or information advantages over the other. Between the conflicts, however, Russia changed how it applied its technological power. Rather than attempting to compete with the US head to head like during the Cold War, in the New Era of Conflict Russia pursued select developments that promised to undermine its opponent's advantages or offered substantive changes to its risk calculus. As a result, during the decade, Russia became a leader in some advanced technologies, such as hypersonics and electronic warfare, and actively competed with the US in others, including artificial intelligence and offensive cyber capabilities. Thus, even while the US continued to lead in technological power writ large, Russia used it selectively to undermine its opponent's strengths, compete in high priority areas, and gain advantages that promised high potential returns on its investments. These findings are summarized in Diagram 17.


Technology
1980s
Enhance Domestic & International Image
Grand Strategy
Offset Strength
Rewards & Punishments
Threat Perceptions, Resource Access, & Strategic Culture
Pressure FPE
NEC
Enhance Domestic & International Image
Grand Strategy
Undercut Sense of Security
Offset Strengths
Threat Perceptions, Resource Access, & Strategic Culture
Deter, Shape, & Demonstrate Power

Comparison of Technology Conflict Models

Diagram 17

Geographically, the two conflict were similar in that the US and Russia actively exploited their advantages and their adversary's vulnerabilities, while also using choke points and strategically important regions to support their grand strategies. One area where the conflicts diverged, however, was cyber technology, which provided increased access to otherwise denied areas and mitigated some of the challenges associated with terrain, borders, and distance. In addition, Russia increased its investments in the Arctic, which it saw as a valuable region for offsetting some US strengths and gaining power. See Diagram 18.


Geography
1980s
Degrade Resource Access & Sense of Security
Impose Costs
Grand Strategy
Threat Perceptions, Resource Access, & Strategic Culture
Hinder Spheres of Influence
Pressure FPE
NEC
Degrade Resource Access & Sense of Security
Offset Strengths RU
Grand Strategy
Impose Costs
Threat Perceptions, Resource Access, & Strategic Culture
Hinder Spheres of Influence
Support Other Elements of Power

Comparison of Geographic Conflict Models

Diagram 18

Collectively, these differences and similarities are summarized in Table 8, below.

Table 8: Summary of Conflicts Similarities & Differences

	Similarities	Differences
Military	Both states used military power, particularly nuclear weapons as a deterrent. Forces were deployed globally to create strategic dilemmas, shape perceptions, & build relationships. Both states used proxies to inflict damage directly & indirectly.	Vast disparity in size of military power during NEC. Russia shifted to small, professional, & technologically advanced force based on a qualitative model. States used cyber technology to conduct direct attacks against other state's interests & homeland with limited attribution.
Economic	Both states employed to coerce, cajole, & shape behaviors. United States' primary tool for directly achieving its objectives. Used sanctions, partnerships, & strong position to exert influence. Russia was the weaker economic power; used espionage to gain advances cheaply.	Russia stabilized & opened economy vs. isolating based on ideological model. During NEC, sought to use system to create alternative financial mechanisms & organizations to offset US power & relationships to balance against it. US increased use of sanctions during NEC. Russia exploited cyber espionage to gain access to greater amounts of sensitive data to support its economic growth.
Information	Both states used information to build their image, support their objectives, & undermine the other's. Espionage & deception played important roles. Russia's primary tool for directly achieving its objectives.	Methods of conducting espionage & active measures differed markedly in terms of scope & degree. NEC saw use of tailored material delivered directly to target populations without reliance on third parties or infiltration. Russia sought not only to deceive the US but to overwhelm the FPE & undermine its domestic control. Data was a new target for manipulation & damage.
Technology	States consistently used technology to support their other elements of power & to burnish their image. The US maintained its general technological lead throughout.	Russia avoided a head to head competition, instead sought advances in new sectors & those that offered high potential pay offs against US strengths.
Geography	Similar approaches in use to undermine other's resource access & sense of security while gaining advantages. States sought to exploit positions and relationships for gain & to pressure SLOCs.	Russia enhanced its position in the Arctic, where the US had under-invested. Both states used cyber to mitigate challenges, such as terrain, distance, & borders when accessing target audiences & infrastructure.

Overall, therefore, the states' approaches to conflict during the two periods had significant similarities and differences that were driven by multiple factors. In the next section, I will analyze the role of the Revolution of Cyber Technology in these developments.

The Impact of the Revolution in Cyber Technology on International Conflict

As demonstrated in the previous section, conflict between Russia and the US underwent some fundamental changes over the past forty years. Whether driven by international stimuli or domestic considerations, this process had a significant impact on state behaviors and how they engaged in the struggle for power. Questions remain, however, as to what caused the changes and the role cyber technology played in the process.

In this section, I will evaluate these questions through three steps. First, to set the foundation for my analysis, I will briefly review the evidence from Chapter Two, with a focus on the cyber-related vulnerabilities. Second, I will synthesize those findings with the conclusions drawn from the above comparative analysis. Through this process, I will conduct a holistic examination that pulls together the cyber-related vulnerabilities, neoclassical realist intervening variables, and state conduct across their elements of power. Finally, based on this analysis, I will draw conclusions and evaluate my hypothesis on how cyber technology has impacted international conflict.

Cyber-Related Vulnerabilities

As discussed in Chapter Two, the Revolution in Cyber Technology brought vast changes to the world. In many ways, these developments were positive, as they greatly improved people's lives. At the same time, however, cyber technology's deep integration created extensive known and unknown vulnerabilities that, if exploited, could impede critical state functions.

To analyze these risks in detail, I examined how an actor might undermine a state's neoclassical realist variables by exploiting its cyber-related physical, economic, social, and governance components (see Table 9). In the process, I found that the resulting vulnerabilities present actors with potentially powerful opportunities to attack target states' decision-making and implementation processes. In addition, while states, businesses, and individuals have taken actions to protect themselves, the extent of the vulnerabilities and their often-hidden nature make complete security an impossible task.

Table 9: Cyber-Related Vulnerabilities

Variables Cyber Components	FPE Perceptions	Ability to access & employ resources	Strategic Culture
Physical Infrastructure (attacks)	Confound stimuli. Create uncertainty on metrics & status of relative power positions.	Slow / complicate production, transportation, GPS, communications, & military capabilities.	Disrupt technology-centric way of war. Create uncertainty on its viability & operational art.
The Economy (attacks; manipulation; espionage)	Undermine real & perceived strengths. Shift economic balance of power.	Damage economy. Manipulate workers. Hinder supply chain. Destroy valuable data.	Deny financial resources required to implement strategy. Impose costs by forcing investments to offset risks.
Society (attacks; manipulation)	Aggravate domestic divisions. Increase threat axes, fear, & distrust.	Manipulate workers, security, & military. Divide & isolate the population & undermine support.	Exacerbate social divisions. Create fear. Raise questions on values & norms.
Government (attacks; manipulation; espionage)	Exacerbate internal divisions. Reinforce FPE biases. Create confusion. Raise questions on relative power.	Hinder bureaucracy. Recruit guerrillas & spies. Undermine elements of power.	Muddle assessments on strategic successes & failures. Inject false indicators.

At the same time, however, vulnerabilities do not equate to successful state exploitation. Thus, questions remain as to whether and how the US and Russia have been using these opportunities and what that tells us about how and why international conflict has changed. The next two sections will focus on these questions.

Synthesis of Vulnerabilities, Variables, & State Conduct

To understand the role cyber technology played during the New Era of Conflict, we must examine whether states exploited the vulnerabilities outlined above. As we look at the list of cyber-related activities and compare them to the risks posed by the deep integration of cyber technology, at least four overlaps become evident.

First, the states actively used cyber technology to create confusion and confound stimuli to a degree that was previously impossible to achieve. This was especially true of Russia, which engaged in an enduring campaign against the US and its allies to surreptitiously overwhelm decision-makers with vast amounts of questionable information, exploit biases, and undermine the FPE's sense of how to employ the state's elements of power in response. This is aptly demonstrated by Russia's tampering with the 2016 elections and associated operations designed to undermine processes and sow doubt across the US government (DNI 2017; Giles 2016). Moreover, despite the United States' extensive military and economic advantages, its reaction was largely ineffectual, which raises fundamental questions about traditional measurements of power.

Second, both the US and Russia invested heavily in offensive cyber tools that threatened the other state's military capabilities and undermined its perceptions of strength. This highlighted extensive possible vulnerabilities and forced the states to make substantial expenditures to offset the associated risks. As a result, the states challenged the other's ability to defend itself and project power, which imposed economic and psychological costs.

Third, the states used cyber technology to conduct extensive attacks against each other. Although these were often conducted in support of espionage and influence operations, they nonetheless exposed the vulnerability of data and infrastructure to harm. Considering its critical importance to digital operating systems, often-sensitive nature, and high value as a global commodity, data's destruction or manipulation poses a serious risk to affected businesses, people, platforms, and government organizations. Thus, cyber technology added another dimension to conflict that extends beyond the traditional threat of tangible physical destruction or economic losses.

Finally, and arguably of greatest consequence, both the US and Russia exploited cyber technology's ubiquity and global reach to directly communicate with and manipulate each other's domestic populations. This was particularly true of Russia, which leveraged the United States' open society to aggravate racial, ethnic, gender, and political fault lines through extensive, targeted social media campaigns. To support these efforts, Russia also engaged in hacking operations that provided access to sensitive data, which it released selectively and strategically.

Adding to these negative effects, the operations' limited attributability undermined the US government's ability to clearly identify the culprit, which would have helped to mitigate the damage, define legal justifications, and provide planning criteria for the responses. Collectively, these factors greatly facilitated and expanded the scope and impact of Russia's active measures programs, which allowed it to harm the United States' domestic unity, undercut its societal norms, tarnish its international image, and create complex challenges for its FPE with little relative cost. While the US also engaged in some of these activities, the available evidence indicates it acted on a much smaller scale due to normative, legal, and political concerns.

Taken together, these developments demonstrate that the US and Russia actively exploited most of the cyber-related vulnerabilities resident within each neoclassical realist variable. This is reflected in Table 10.

Table 10: Exploited Cyber-Related Vulnerabilities

Variables Cyber Components	FPE Perceptions	Ability to access & employ resources	Strategic Culture
Physical Infrastructure (attacks)	Confound stimuli. Create uncertainty on metrics & status of relative power positions.	Slow / complicate communications & military capabilities.	Disrupt technology-centric way of war. Create uncertainty on its viability & operational art.
The Economy (attacks; manipulation; espionage)	Undermine real & perceived strengths.	Destroy valuable data.	Impose costs by forcing investments to offset risks.
Society (attacks; manipulation)	Aggravate domestic divisions. Increase threat axes, fear, & distrust.	Divide & isolate the population & undermine support.	Exacerbate social divisions. Create fear. Raise questions on values & norms.
Government (attacks; manipulation; espionage)	Exacerbate internal divisions. Reinforce FPE biases. Create confusion. Raise questions on relative power.	Hinder bureaucracy. Undermine elements of power.	Muddle assessments on strategic successes & failures. Inject false indicators.

While this analysis provides important data on how the states exploited cyber technology, to fully understand their impacts on the New Era of Conflict, the above findings must be synthesized with the results of the similarities and differences analysis from previous section. This process leads to three main conclusions.

First, in the New Era of Conflict cyber technology provided the US and Russia with the ability to execute unique activities, such as limited attribution attacks against the other’s homeland and operations to destroy, steal, and manipulate sensitive data. Although destructive attacks were possible during the 1980s, there is no reliable evidence that the states conducted sabotage operations against the other’s territory or military forces. In addition, while computers were used extensively in the private and public sectors during the Cold War, the lack of a global, interconnected network prevented their access except through risky clandestine operations involving physical human presence. Moreover, since data had yet to become the invaluable commodity that it was during the New Era of Conflict, states had limited reasons to pursue it. As such, cyber technology not only expanded the state's abilities to conduct direct attacks, it also created a new category of targets to manipulate, steal, damage, or destroy.

Second, cyber technology dramatically enhanced the United States' and Russia's ability to conduct traditional activities, which they executed on a much broader scope, to a greater degree, and with much more effectiveness than previously possible. Specifically, by leveraging cyber connectivity as well as advances in graphic design, video editing, navigation, communications, and data analytics, the US and Russia manifestly expanded their capabilities in multiple areas, including espionage, sabotage, deception, long-range precision targeting, and propaganda operations.

Finally, the advent of cyber technology established a new, vast domain for conflict that brought together a unique blend of cognitive, virtual, and physical components. In response, the states developed a distinctive sector of offensive and defensive capabilities that evolved rapidly, were intangible and secretive in nature, and had real impacts across the states' vulnerabilities. As a result, a new venue of conflict emerged in which it was increasingly difficult to count weapons, assess their capabilities, and develop appropriate countermeasures. In context with the tremendous capabilities the new technology offers, these changes greatly complicated the metrics of power and raised important questions about its meaning in the Twenty-first Century.

Collectively, this analysis demonstrates that cyber technology has changed international conflict in fundamental ways. As a domain with unique characteristics, global ubiquity, and deep integration into nearly every facet of the modern state, cyberspace and its associated technology provided the US and Russia with the opportunity to create previously impossible effects, with lower risk, and to an unprecedented degree. In the next section, I will use these findings and their supporting evidence to evaluate my hypothesis.

Assessing the Hypothesis

As outlined in the initial chapter, my theory is that the revolution in cyber technology is changing international conflict by providing external actors the unprecedented ability to directly penetrate states and undermine their power through novel, rapidly evolving, globally capable, and minimally attributable methods. As a result, the meaning of power has shifted from a material-centered concept to one that is more nuanced and difficult to measure.

To examine this theory, I will look at its two assertions in turn. First, is the question of whether cyber technology allowed external actors to directly interfere with the states' exercise of power in unique ways. As detailed in the previous sections, the US and Russia used cyber technology to exploit multiple vulnerabilities in their opponent's intervening variables. While both states attempted to create similar effects in the 1980s, the ways and means offered were risky, laborious, and of limited impact. Cyber-enabled operations, however, were not only more extensive in degree and scope but also presented less risk than the traditional human-centric options. In addition, due to cyber technology, the US and Russia were able to directly target their adversary in ways they were unable or unwilling during the Cold War. Thus, the first element of my hypothesis is valid.

Second, is the question of the how the states' use of cyber technology influenced the metrics of international power. As discussed in the previous section, the technology not only has demonstrated value as a tool for creating effects across the neoclassical realist intervening variables, but it is also a rapidly evolving, intangible domain with capabilities and potential impacts that are powerful yet difficult to quantify. Thus, unlike with traditional metrics, such as economic performance and military hardware, in a cyber-enabled world it is difficult for states to fully understand their relative power positions.

Moreover, while some scholars argue that the technology's impacts are overstated, this study's findings demonstrate the exact opposite, as cyber has become a great facilitator and major operating domain for modern international conflict. As a result of the attending vulnerabilities and capabilities, states now have a venue in which to use their elements of power to create substantial effects across their adversaries' neoclassical vulnerabilities with limited accountability. In the process, information and technology have become distinctly more powerful tools that, while not replacing military and economic means, have nonetheless grown greatly in importance. For the realist school of thought, in which relative material power is the centerpiece of international relations, these less quantifiable and intangible capabilities create serious challenges.

Taken together, these conclusions indicate that the hypothesis is valid, as cyber technology has dramatically changed international conflict, enhanced states' ability to directly impact others' vulnerabilities, and created fundamental challenges to the meaning of power in the 21st Century. In the next section, I will examine these findings' implications and discuss the study's limitations, gaps, and areas for further research.

Gaps, Further Research, and Implications

In the previous chapters, I conducted a detailed analysis of the grand strategies the US and Russia employed in two conflicts over the past forty years. This process involved an examination of numerous documents reflecting the states' goals and the actions they undertook to achieve them. In addition, I provided an extensive assessment of cyber technology's deep integration into states' governance and social fabric and identified some critical vulnerabilities this created. Once the cases were compared and the evidence synthesized, the resulting data provided the foundation for my subsequent analysis, which demonstrated that cyber technology has changed international conflict in several important ways.

In this section, I will complete this study by identifying gaps and highlighting areas for additional research. In addition, I will discuss the broader implications of my findings, which extend beyond the impacts of cyber technology to include the nature of modern conflict and the United States' responses thereto.

Gaps and Further Research

Despite this project's extensive empirical foundation, it nonetheless contains several gaps that warrant further research. First, grand strategy is a controversial concept, which raises questions about its utility as the dependent variable and overall yardstick for measuring international conflict (Brands 2014: 3). Moreover, my findings on the US and Russian strategies are open to challenge, as the literature reflects a range of perspectives on what they were or if they even existed (Dombrowski & Reich 2018; Zubok 2010; Wilson 2007). While I have mitigated these risks by clearly defining my dependent variable and accounting for evolution in the individual administration’s approaches, additional research is necessary to determine whether an alternative method would yield different results.

Second, the project faced limitations on data availability, particularly due to classified material and other government restrictions. This was exacerbated by my inability to travel and a lack of Russian language skills. Together, these hinderances generally limited my evidence to that available online or contained in secondary sources. Although archives’ digitization of their holdings and online translation capabilities mitigated these challenges, additional research involving physical access and more Russian documents would further improve the project’s empirical foundations.

Third, since the study analyzed two great power states during two periods of conflict, its generalizability is limited. This is particularly true of China, which has distinct historical experiences, a different way of engaging in international conflict, and may have employed cyber technology in unique ways to achieve its goals. Moreover, the study’s conclusions likely have limited applicability to small and medium powers. As such, research involving additional cases, especially China, would greatly enhance the study’s empirical strength and utility.

Finally, the study did not conduct a complete analysis of the factors that generated change in the states’ grand strategies over time. While such an approach would be limited by the inherently complex and multidirectional causal forces at play, it would nonetheless help to highlight some of the most important factors influencing state behaviors. In the process, the analysis would enhance our understanding of international conflict and may further shape the study’s conclusions on cyber technology’s impacts.

Implications

Although this project's primary research question focused on cyber technology, at its core the study's purpose was to gain a better understanding of international conflict in the Twenty-First Century. Through my examination of the US and Russian modes of conflict, therefore, I identified significant differences between conflict in the 1980s and the New Era that raise several important implications.

First, it is evident that my hypothesis was too limited, as cyber technology has had a much broader impact than initially appreciated. Specifically, not only has it enabled states to have direct and indirect effects inside the others' borders, but cyber technology also created ripple effects across all the elements of power. In the process, it greatly enhanced weapons' range and precision, improved decision making and communications, provided extensive economic advantages, served as the backbone for dramatic technological advancements, and changed navigation and communications in unparalleled ways. Thus, the impact of cyber technology on international conflict reaches well beyond cyber-based attacks, espionage, and influence operations, to touch on essentially every component of the modern state's national security and its associated resources, organizations, and processes.

Second, and central to this study, cyber technology created a new domain for conflict, unlike any that had yet existed. As a result, targets for attack, theft, and influence now expand globally and include not only the physical and cognitive spheres, but also virtual elements such as data and digital environments. Moreover, this new domain is essentially global in scale and is integrated into every element of power. For the US national security community, which is geographically oriented and imbued with a strategic culture focused on quantitative metrics, these realities raise fundamental questions on how to assess threats and opportunities, prioritize elements of power, develop appropriate policies, and make the requisite resource investments.

Third, it is apparent that, between the US and Russia, the latter was much more successful in developing an effective grand strategy. Specifically, rather than attempting to engage in a head to head fight against the United States' fortes, Russia improvised by developing sufficient military and economic power to provide a strong deterrent, safeguard the regime at home and abroad, and ensure that it could achieve its other objectives. At the same time, Russia also developed its information, technology, and geographical capabilities specifically to offset US strengths in some areas, gain a lead in others, and inflict costs on its opponent's vulnerabilities with limited risk. Thus, Russia adopted an offensively and defensively balanced strategy that exploited the United States' open society and bureaucratic structure to impose costs and undermine its power while largely negating its strengths.

Even though the US has slowly woken up to these challenges and made some adjustments in response, it has nonetheless largely failed to fully appreciate and adapt to Russia's way of conflict. Instead, the US has continued to follow its Cold War strategy of attempting to deter Russia with overwhelming military and economic power while using its other elements to impose costs and offset its influence. Although this approach has created some negative effects for Putin and the Russian FPE writ large, available evidence indicates that it has been highly expensive but largely ineffective in achieving US goals. Furthermore, US administrations have often played into Russia's hands by exploiting the state's own domestic and bureaucratic divisiveness for political gain. Thus, rather than aptly assessing the threat and defending against it, the FPE instead exacerbated the acrimony, fed the Russian narrative, and facilitated its adversary's strategic successes.

Collectively, these findings demonstrate that the US National Security Community's approach to international conflict in the Twenty-First Century is generally lacking in imagination, critical thinking, and clear-eyed analysis. Thus, rather than grasping Russia's strategy and aptly responding to it, the US FPE has deferred to prohibitively expensive deterrence models based on archaic planning assumptions and outdated metrics of power. As a result, the US has failed to adapt, preferring instead to pour vast sums of money into a modern version of the Maginot Line that Russia has aptly avoided through its new way of conflict (McChrystal 2015: 51-52).

Conclusion

From its nascent days as a fragile link between two computers to a multifaceted, global system with billions of users and connected devices, cyber technology has become an invaluable asset for most governments, businesses, and societies. As its components have shrunk in size and grown in capability, it has also infiltrated nearly every facet of our daily lives. In the process, cyber technology has changed how we communicate, work, travel, and engage in financial transactions, and it has also altered how states interact with individuals, organizations, and each other.

While these developments have brought great benefits, they have also had negative effects, as state and non-state actors have exploited the technology's vast vulnerabilities, deep integration, and critical importance for their own gains. At the international level, this trend has been pronounced, as Russia, China, the United States, Iran, Pakistan, India, and North Korea, among others, have used cyber technology to steal information, manipulate data, attack their adversaries, and create domestic turmoil across borders. As a result, cyber technology has become a topic of increased interest for scholars, who have written a myriad of works analyzing how it is impacting international relations.

Despite the volume of material, however, the scholarship on cyber technology is largely focused on narrow aspects of its real and potential effects. In addition, scholars' findings reflect a range of thought, with differences often generated by a lack of definitional discipline or dissimilarities in the topics of analysis. As a result, the literature fails to provide a holistic, empirical analysis of how the technology is influencing international relations.

This project attempted to fill part of the gap by examining cyber technology's impact on international conflict. To ensure consistency and avoid a narrow focus on war, the study defined conflict broadly as the adversarial struggle among actors to achieve their objectives within the international system. In addition, for a theoretical foundation, the study used neoclassical realism, drawn primarily from Ripsman, Taliaferro, and Lobell's 2016, *Neoclassical Realist Theory of International Relations*. This framework, which posits the imposition of intervening variables in the causal chain between international stimuli and grand strategy formation, provided the framework for my analysis of state behaviors. In addition, in applying the theory, I argued that the intervening variables, which form an essential component of a state's grand strategy development and implementation process, present important targets for attack and influence. If an adversary can influence these variables, therefore, it can impact a state's ability to act.

Methodologically, I used a comparative case study approach in which I examined the grand strategies adopted by the United States and Russia during the 1980s and the 2007-2018 timeframe. By analyzing and then comparing how the states attempted to use their elements of power to influence the other's neoclassical intervening variables in pre and post-cyber periods, and then comparing the results, I was able to identify key differences between the conflicts. These results I then synthesized with a list of cyber-related vulnerabilities and specific state practices to demonstrate how the US and Russia have used cyber technology to achieve their goals in unique ways.

Based on this process, I reached three important conclusions. First, I found that cyber technology has had a fundamental impact on international conflict by providing states with the ability to create direct and indirect effects on their adversaries' decision-making and implementation processes to a unique scope and degree. Second, while the effects can be destructive in nature, states also have the demonstrated ability to leverage cyber technology to inflict non-material harm on others' governance, social, physical, and economic functions. Thus, the effects reach well beyond cyberattacks, which is where many scholars have focused. Finally, since cyber capabilities are largely unquantifiable and non-tangible, the meaning of power has changed from a material-centric concept to one that is more nuanced and difficult to measure. This has impacted states' means of engaging in conflict and greatly complicated the calculation of relative power in the international system. Collectively, these findings validate my initial hypothesis.

In addition to the above, however, I also reached other important conclusions on international conflict in the Twenty-First Century. Specifically, the comparative analysis between Russia and the United States in the New Era of Conflict (2007-2018), demonstrated that, while the former has been highly effective in incorporating cyber technology into its grand strategy, the latter has not. Instead, despite its status as a global technical leader, the United States has largely followed a Cold War style deterrence model, in which material metrics of power dominate.

Moreover, I found that Russia has adeptly acted to offset US strengths and attack its vulnerabilities in ways the United States FPE has been slow to recognize and respond to effectively. As a result, while Russia has used military resources to deter the US from imposing unacceptable costs, it has simultaneously employed its other elements of power to undermine the United States' domestic unity, strategic flexibility, economic influence, and international prestige. While not all these activities have been successful and they also generated significant costs, the Russian strategy has nonetheless been highly effective in achieving its overarching goals.

Although these findings raise fundamental questions about modern international conflict, the study has several gaps that warrant further analysis. As such, additional research involving more cases, a different methodology, and an expanded set of sources would greatly enhance our understanding of whether the above conclusions are apt and generalizable. In addition, applying different theoretical models from other schools of thought would further test and expand the results.

Gaps aside, this study nonetheless presents a strong, empirically based argument that cyber technology has changed modern international conflict in fundamental ways. While many questions remain and further analysis is necessary, it is evident that material metrics of power are useful but can no longer serve as the centerpiece for understanding international relations or measuring strategic success. Thus, in the Twenty-First Century, states must recognize that international conflict will not be driven primarily by the quantitative superiority of their militaries or the relative size of their economies, but will also be greatly impacted by much less tangible aspects of power that they ignore or downplay to their detriment.

Bibliography

Abbate, Janet. 2010. "Privatizing the Internet: Competing Visions and Chaotic Events, 1987-1995)." *IEEE Annals of the History of Computing.* January-March: 10-22.

---. 1999. *Inventing the Internet* (Cambridge: MIT Press).

Adamsky, Dmitry. 2019. "How the Russian Church Learned to Stop Worrying and Love the Bomb: Orthodoxy's Influence on Moscow's Nuclear Complex." *Foreign Affairs* June 14. https://www.foreignaffairs.com/articles/russian-federation/2019-06-14/how-russian-church-learned-stop-worrying-and-love-bomb (accessed January 20, 2020).

Adat, Vipindev and B.B. Gupta. 2017. "Security in Internet of Things: issues, challenges, taxonomy, and architecture." *Telecommunication Systems* 67: 423-441.

Adomeit, Hannnes. 2018. "Putin's 'Greater Russia': misunderstanding or mission?" *Raamop Rusland* (*Window on Russia)*. 27 February. https://www.raamoprusland.nl/dossiers/roesski-mir/878-putin-s-greater-russia-misunderstanding-or-mission (accessed December 22, 2019).

Alarid, Maeghin. 2009. "Recruitment and Radicalization: The Role of Social Media and New Technology." In *Impunity: Countering Illicit Power in War and Transition* eds. Michelle Hughes and Michael Miklaucic (London: Routledge).

Alger, John I. 1982. *The Quest for Victory: The History of the Principles of War* (Westport: Greenwood Press).

Aliyev, Nurlan. 2019. "Russia's Military Capabilities in the Artic." International Centre for Defence and Security. https://icds.ee/russias-military-capabilities-in-the-arctic/ (accessed January 11, 2020).

Allen, Robert C. 2001. "The rise and decline of the Soviet economy." *Canadian Journal of Economics* 34(4): 859-881.

Ali, F. B. 2009. "The Principles of War." *Royal United Services Institutions* 108(630): 159-165.

Allcott, Hunt and Matthew Gentzkow. 2017. "Social Media and Fake News in the 2016 Election." *Journal of Economic Perspectives* 31(2): 211-236.

Anderson, Jim. "Soviet aid to Cuba: $11 million a day." *UPI*. June 18. https://www.upi.com/Archives/1983/06/18/Soviet-aid-to-Cuba-11-million-a-day/2328424756800/

Anderson, Monica, Andrew Perrin, Jinjing Jiang, and Madhumitha Kumar. 2019. "10% of American's don't use the internet. Who are they?" April 22. Pew Research Center.

https://www.pewresearch.org/fact-tank/2019/04/22/some-americans-dont-use-the-internet-who-are-they/ (accessed May 1, 2019).

Andropov, Yuri Vladimirovich. 1982. “Report on the Work of the Committee on State Security of the USSR for 1981.” April 13. https://digitalarchive.wilsoncenter.org/document/112803 (accessed October 04, 2019).

---. 1981. “Report Made at the KGB Party Caucus Meeting by Yu. V. Andropov, ‘The Results of 26th Congress of the CPSU and Tasks for the Party Organization of the KGP That Ensue from the CPSU Congress’ Decisions and the CPSU Central Committee Report.’” Trans. Angela Greenfield. https://digitalarchive.wilsoncenter.org/document/176633#_ftn1 (accessed October 04, 2019).

Anthony, Ian. 1998. “Economic Dimensions of Soviet and Russian arms exports.” In Ian Anthony, ed. *Russia and the Arms Trade* (Oxford: Oxford University Press).

Arquilla, John and David Ronfelt, ed. 1997. *In Athena’s Camp: Preparing for conflict in the information age* (Santa Monica: RAND).

Atkinson, Tyler, David Luttrell, and Harvey Rosenblum. 2013. *Staff Paper: How Bad Was It? The Costs and Consequences of the 2007-09 Financial Crisis* (Dallas: Federal Reserve Bank of Dallas).

Atzori, Luigi, Antonio Iera, and Giacomo Morabito. 2016. “Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm.” *Ad Hoc Networks* 56: 122-140.

AV-Test. 2019. “Malware.” https://www.av-test.org/en/statistics/malware/ (accessed May 9, 2019).

Avgerinos, Katherine P. 2009. “Russia’s Public Diplomacy Effort: What the Kremlin is Doing and Why It’s not Working.” *Journal of Public and International Affairs* 20: 115-132.

Babayan, Nelli. 2015. “The return of the empire? Russia’s counteraction to transatlantic democracy promotion in its near abroad.” *Democratization* 22(3): 438-458.

Bandow, Doug. 2020. “How Our Economic Warfare Brings the World to Heel.” CATO Institute. https://www.cato.org/publications/commentary/how-our-economic-warfare-brings-world-heel (accessed March 15, 2020).

Banks, William. 2017. “State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0.” *Texas Law Review 95*: 1487-1513.

Balzacq, Thierry, Peter Dombrowski, and Simon Reich. 2018. “Is Grand Strategy a Research Program? A Review Essay.” *Security Studies.* 1-29.

Baran, Paul. 1964. *Memorandum RM-3767-PR, On Distributed Communications: XI. Summary Overview* (Santa Monica: RAND). https://www.rand.org/pubs/research_memoranda/RM3767.html (accessed April 8, 2019).

Barany, Zoltan. 2007. *Democratic Breakdown and the Decline of the Russian Military* (Princeton: Princeton University Press).

Barsky, Robert B. and Lutz Kilian. 2001. “Do We Really Know that Oil Caused the Great Stagflation? A Monetary Alternative.” *Microeconomics Annual* 16: 137-183.

Bartosh, Alexander. “Russia cannot escape hybrid wars: Multidimensional Armed Conflict and National Security.” March 09. http://nvo.ng.ru/concepts/2018-03-09/1_987_hybridwar.html (accessed March 27, 2020).

Batchelor, James. 2018. “GamesIndustry.biz presents . . . The Year In Numbers 2018.” https://www.gamesindustry.biz/articles/2018-12-17-gamesindustry-biz-presents-the-year-in-numbers-2018 (accessed May 1, 2019).

Bennett, Andrew and Jeffrey T. Checkel. 2015. *Process Tracing: From Metaphor to Analytic Tool* (Cambridge: Cambridge University Press).

Béraud-Sudreau, Lucie and Nick Childs. 2018. “The US and its NATO allies: costs and value.” International Institute for Strategic Studies. July 9. https://www.iiss.org/blogs/military-balance/2018/07/us-and-nato-allies-costs-and-value (accessed February 22, 2020).

Bergen, Peter and Katherine Tiedemann. 2011. “Washington’s Phantom War: The Effects of the U.S. Drone Program in Pakistan.” *Foreign Affairs* (July/August) https://www.foreignaffairs.com/articles/pakistan/2011-07-01/washingtons-phantom-war (accessed February 08, 2020).

Berrios, Ruben. 1988. *#227: Soviet-Latin American Economic Relations* (Washington, DC: Wilson Center).

Bērziņa, Ieva. 2014. *Color Revolutions: Democratization, Hidden Influence or Warfare?* (Riga: National Defence Academy of Latvia, Center for Security and Strategic Research) https://www.naa.mil.lv/sites/naa/files/document/1_WP2014%20Color%20revolutions.pdf (accessed December 07, 2019).

Blank, Stephen. 2008a. “Russia and the Black Sea’s Frozen Conflicts in Strategic Perspective.” *Mediterranean Quarterly* 19(3): 23-54.

---. 2008b. “Web War I: Is Europe’s First Information War a New Kind of War?”, *Comparative Strategy* 27(3): 227–47.

Blank, Stephen and Younkyoo Kim. 2016. “Economic Warfare a la Russe: The Energy Weapon and Russian National Security Strategy.” *The Journal of East Asian Affairs* 30.1: 1-39.

Blumberg, Stephen J. and Julian V. Luke. *Wireless Substitution: Early Release of Estimates From the National Health Interview Survey, January – June 2018* (Washington, DC: National Center for Health Statistics).

Boehm, Sharla and Paul Baran. 1964. *RM-3103-PR, On Distributed Communications: II Digital Simulation of Hot-Potato Routing in a Broadband Distributed Communications Network* (Santa Monica: RAND). https://www.rand.org/pubs/research_memoranda/RM3103/RM3103 .pubs.html (accessed April 28, 2020)

Boese, Wade. 2008. "Bush, Putin Leave Arms Disputes Unsettled." *Arms Control Today* 38(4): 27-28.

Boghardt, Thomas. 2009. "Soviet Bloc Intelligence and Its AIDS Disinformation Campaign." *Studies in Intelligence* 53(4): 1-24.

Boston, Scott, Michael Johnson, Nathan Beauchamp-Mustafaga, and Yvonne K. Crane. 2018. *Assessing the Conventional Force Imbalance in Europe: Implications for Countering Russian Local Superiority* (Santa Monica: RAND).

Bouwmeester, Han. 2017. "Lo and Behold: Let the Truth Be Told – Russian Deception Warfare in Crimea and Ukraine and the Return of 'Maskirovka' and 'Reflexive Control Theory.'" In Paul A.L. Ducheine and Frans P.B. Osinga. Ed. *Netherlands Annual Review of Military Studies* (The Hague: T.M.C. Asser Press): 125-153.

Boyes, Hugh. 2015. "Cybersecurity and Cyber-Resilient Supply Chains." *Technology Innovation Management Review* 5(4): 38-34.

Brand, Stewart. 2001. "Founding Father." *Wired.* https://www.wired.com/2001/03/baran/ (accessed April 8, 2019).

Brands, Hal. 2016. "Barack Obama and the Dilemmas of American Grand Strategy." *The Washington Quarterly* 39(4): 101-125.

---. 2014. *What Good is Grand Strategy? Power and Purpose in American Statecraft from Harry S. Truman to George W. Bush* (Ithaca: Cornell University Press).

Brezhnev, Leonid. 1982. "The Military Strength of the State." *Vital Speeches of the Day* 49(3): 66-67.

---. 1979. "American Nuclear Missile Weapons in Western Europe." *Vital Speeches of the Day* 46(2): 34-36.

Brinkley, Douglas. 2007. *The Reagan Diaries* (New York: Harper Perennial).

Brodie, Bernard. 1949. "Strategy as a Science." *World Politics* 1(4): 467-488.

Brooks, Stephen G. and William C. Wohlforth. 2016. *America Abroad: The United States' Global Role in the 21st Century* (New York: Oxford University Press).

Burns, William J. 2019. "How the U.S.-Russian Relationship Went Bad: An American diplomat tells the inside story of Yeltsin, Putin, and opportunities lost." *The Atlantic* (April). https://www.theatlantic.com/magazine/archive/2019/04/william-j-burns-putin-russia/583255/ (accessed February 19, 2020).

Cailliau, Robert and James Gillies. 2012. "How the world wide web was won." *OECD Observer* 293: 32-33.

Caplan, Nathalie. 2013. "Cyber War: the Challenge to National Security." *Global Security Studies* 4 (Winter): 93-115.

Carbon Black. 2019. *Global Threat Report: Year of the Next-Gen Cyberattack.* January. https://www.carbonblack.com/resources/threat-research/year-of-the-next-gen-cyberattack/ (accessed April 28, 2020)

Carpenter, Ted Galen. 2019. *Gullible Superpower: US Support for Bogus Democratic Movements* (Washington, DC: CATO).

Castelluccio, Michael. 2018. "Toward Web 3.0." *Strategic Finance* December: 53-54).

Cebrowski, Arthur K. Vice Admiral. 2005. "Foreward." In Anthony D. McIvor, ed. *Rethinking the Principles of War* (Annapolis: Naval Institute Press).

Center for Strategic and International Studies (CSIS). 2020. "Russia Sanctions Tracker." https://russiasanctionstracker.csis.org/ (accessed February 22, 2020).

---. 2019. *Significant Cyber Incidents Since 2006* (Washington, DC: CSIS). https://csis-prod.s3.amazonaws.com/s3fs-public/190211_Significant_Cyber_Events_List.pdf (accessed May 20, 2019).

Central Committee, Communist Party of the Soviet Union (CC CPSU). 1986a. *Session of the Politburo of the CC CPSU (Top Secret Only Copy Working Notes)*. 14 October https://nsarchive2.gwu.edu/NSAEBB/NSAEBB203/Document21.pdf (accessed June 12, 2020).

---. 1986b. "Working Notes: Session of the Politburo of the CC CPSU. Top Secret." 22 October https://nsarchive2.gwu.edu/NSAEBB/NSAEBB203/Document22.pdf (accessed June 12, 2020).

Central Intelligence Agency (CIA). 1989. *Gorbachev's Strategy for Managing the Defense Burden* (Washington, DC: CIA).

---. 1985a. *A Comparison of the US and Soviet Economies: Evaluating the Performance of the Soviet System* (Washington, DC: CIA).

---. 1985b. *Soviet Military Power* (Washington, DC: CIA).

---. 1983. *The Soviet Military Advisory and Training Program for the Third World* (Washington, DC: CIA).

---. 1982. *Soviet Policies and Activities in Latin America and the Caribbean* (Washington, DC: CIA).

---. 1981. *Soviet Support for International Terrorism and Revolutionary Violence* (Washington, DC: CIA).

Cerf, Vint. 1995. "IETF and the Internet Society." July 18. https://www.internetsociety.org/internet/history-of-the-internet/ietf-internet-society/ (accessed April 11, 2019).

Chan, Chi Ling. 2015. "Fallen Behind: Science, Technology, and Soviet Statism." *Intersect* 8(3): 1-11.

Chandler, Adam. 2015. "Russia is Really Just Showing Off in Syria at this Point." *The Atlantic* 07 October. https://www.theatlantic.com/international/archive/2015/10/russia-cruise-missiles-syria/409444/ (accessed January 22, 2020).

Chernayaev, Anatoly. 1986a. "Notes from the Politburo Session." October 8. Trans. Anna Melyakova and Svetlana Savranskaya. The National Security Archive (Source: The Gorbachev Foundation Archive) https://nsarchive2.gwu.edu/NSAEBB/NSAEBB203/Document08.pdf (accessed September 15, 2019).

---. 1986b. "Notes from the Politburo Session." October 30. Trans. Svetlana Savranskaya https://nsarchive2.gwu.edu/NSAEBB/NSAEBB203/Document23.pdf (accessed June 12, 2020).

Chernenko, Konstantin. 1984. "Party and People United." *Vital Speeches of the Day* 50(13): 386-391.

Choucri, Nazli. 2012. *Cyberpolitics in International Relations* (Cambridge: The MIT Press).

Chua, Amy. 2018. "Tribal World: Group Identity is All." *Foreign Affairs* 97(4): 25-33.

Cisco. 2019. "Cisco Visual Networking Index: Forecast and Trends, 2017-2022." February 27. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html#_Toc532256789 (accessed April 30, 2019).

Clark, Joseph Roger. 2019. "Russia's Indirect Grand Strategy." *Orbis* 63(2): 225-239.

Clarke, Michael and Anthony Ricketts. 2017. "Did Obama Have a Grand Strategy?" *The Journal of Strategic Studies* 40(1-2): 295-324.

Clarke, Richard A. and Robert K. Knake. 2010. *Cyber War* (New York: HarperCollins).

Cline, Jay. 2017. "Pulse Survey: GDPR budgets top $10 million for 40% of surveyed companies." Price, Waterhouse, and Cooper. https://www.pwc.com/us/en/services/consulting/%20library/general-data-protection-regulation-gdpr-budgets.html (accessed May 16, 2019).

Cline, Ray S. 1987. "Introduction to Basic Soviet Geopolitics. In Cline, Ray S., James Arnold Miller, and Roger E. Kanet, Eds. *Asia in Soviet Global Strategy* (Boulder: Westview Press).

Cohen, Ariel and Robert E. Hamilton. 2011. *The Russian Military and the Georgia War: Lessons and Implications* (Carlisle: Strategic Studies Institute).

Collins, Gabriel. 2017. "Rice University's Baker Institute for Public Policy, Issue Brief: Russia's Use of the 'Energy Weapon' in Europe." https://www.bakerinstitute.org/media/files/files/%20ac785a2b/BI-Brief-071817-CES_Russia1.pdf (accessed January 18, 2020).

Collins, John M. and Elizabeth Ann Severns. 1981. *Report No. 81-233 S: U.S. / Soviet Military Balance Statistical Trends, 1970-1980* (Washington, DC: CRS).

Collins, Joseph J. "The Soviet Invasion of Afghanistan: Methods, Motives, and Ramifications." *Naval War College Review* 33(6): 53-62.

Congressional Budget Office (CBO). 2014. “Appendix H: Historical Budget Data.” *The Budget and Economic Outlook: 2014-2024* (Washington, DC: CBO) https://www.cbo.gov/sites/default/%20files/%20cbofiles/%20attachments/45010-breakout-AppendixH.pdf (accessed June 30, 2019).

Congressional Research Service (CRS). 2020. “U.S. Sanctions on Russia.” CRS Report R45415. January 17. https://crsreports.congress.gov/product/pdf/R/R45415/9 (accessed February 23, 2020).

---. 2019. *U.S. Sanctions on Russia* (Washington, DC: Congressional Research Service).

Conley, Heather A. 2019. “The Implications of U.S. Policy Stagnation toward the Arctic Region.” Center for Strategic & International Studies. May 3. https://www.csis.org/%20analysis/implications-us-policy-stagnation-toward-arctic-region (accessed March 3, 2020).

Cooley, Alexander. 2012. “The New Great Game in Central Asia: Geopolitics in a Post-Western World.” *Foreign Affairs*. August 7. https://www.foreignaffairs.com/articles/central-asia/2012-08-07/new-great-game-central-asia (accessed March 7, 2020).

The Council of Economic Advisers. 2018. “The Costs of Malicious Cyber Activity to the U.S. Economy.” https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf (accessed May 16, 2019).

Council on Foreign Relations. 2020. “Cyber Operations Tracker.” https://www.cfr.org/%20interactive/cyber-operations (accessed March 3, 2020).

---. 2018. “Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms.” February 23. https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms (accessed April 30, 2019).

---. 2017. “Maintaining U.S. Leadership on Internet Governance.” February 21. https://www.cfr.org/report/maintaining-us-leadership-internet-governance (accessed March 22, 2020).

Covington, Stephen R. 2016. *The Culture of Strategic Thought Behind Russia’s Modern Approaches to Warfare* (Cambridge: Belfer Center for Science and International Affairs).

The Critical 5. 2015. “Role of Critical Infrastructure in National Prosperity: Australia, Canada, New Zealand, United Kingdom, and United States Shared Narrative.” October. https://www.cisa.gov/publication/critical-five-shared-narrative-2015?topic=cybersecurity (accessed May 15, 2019).

Cybersecurity and Infrastructure Security Agency (CISA). 2019a. “Critical Infrastructure Sectors.” https://www.cisa.gov/critical-infrastructure-sectors (accessed May 15, 2019).

---. 2019b. “National Critical Functions Set.” https://www.cisa.gov/national-critical-functions-set (accessed May 16, 2019).

---. 2019c. “What Does CISA do?” https://www.cisa.gov/ (accessed May 15, 2019).

Daalder, Ivo H. and James M. Lindsay. 2018. “The Committee to Save the World Order: America’s Allies Must Step Up as America Steps Down.” *Foreign Affairs* (November / December). https://www.foreignaffairs.com/articles/2018-09-30/committee-save-world-order (accessed March 14, 2020).

Daly, John C.K. 2015. “Russia Shutters Northern Distribution Network.” The Jamestown Foundation 12(111). https://jamestown.org/program/russia-shutters-northern-distribution-network/ (accessed March 8. 2020).

Davis, John S. II, Benjamin Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, Michael S. Chase. 2017. *Stateless Attribution: Toward International Accountability in Cyberspace* (Santa Monica: RAND). https://www.rand.org/pubs/research_reports/RR2081.html (accessed May 20, 2019).

DeBrusk, Chris and Paul Mee. 2018. “Cyber Risks that Hide in Plain Sight.” Oliver Wyman. https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/%20june/Cyber-Risks-That-Hide-In-Plain-Sight.pdf (accessed May 16, 2019).

Deloitte. 2019. “2019 Media & Entertainment Industry Outlook.” https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/%20media-and-entertainment-industry-outlook-trends.html (accessed May 1, 2019).

Dennis, Steve. 2018. “E-Commerce May Be Only 10% of Retail, But That Doesn’t Tell the Whole Story.” *Forbes* April 9. https://www.forbes.com/sites/stevendennis/2018/04/09/e-commerce-fake-news-the-only-10-fallacy/#6fe7381339b4 (Accessed April 16, 2019).

Deudney, Daniel and G. John Ikenberry. 2018. “Liberal World: The Resilient Order.” *Foreign Affairs* 97(4): 16-24.

Dombrowski, Peter and Simon Reich. 2018. “Beyond the Tweets: President Trump’s Continuity in Military Operations.” *Strategic Studies Quarterly* 12(2): 56-81.

---. 2017. “Does Donald Trump have a grand strategy?” *International Affairs* 93(5): 1013-1037.

DOMO, Inc. 2019. *Data Never Sleeps 6.0.* https://www.domo.com/learn/data-never-sleeps-6 (accessed April 11, 2019).

Donaldson, Robert H. and Joseph L. Nogee. 2009. *The Foreign Policy of Russia: Changing Systems, Enduring Interests*. 4th Ed. (Armonk: M.E. Sharpe).

Doyle, Michael. 1983. “Kant, Liberal Legacies and Foreign Affairs.” *Philosophy and Public Affairs* 12(3): 205-235.

Drezner, Daniel. 2011. “Does Obama have a grand strategy.” *Foreign Affairs* 90(4). https://www.foreignaffairs.com/articles/2011-06-17/does-obama-have-grand-strategy (accessed February 12, 2019).

Drum, Kevin. “Tech World: Welcome to the Digital Revolution.” *Foreign Affairs* 97(4): 43-48.

D'Souza, Dinesh. 2003. “How the East was Won.” *American History* 38(4): 36-43.

Dueck, Colin. 2015. *The Obama Doctrine: American Grand Strategy Today* (Oxford: Oxford University Press).

Dunbabin, J.P.D. 1994. *International Relations Since 1945, A History in Two Volumes. The Cold War Years: The Great Powers and Their Allies* (London: Longman Group).

Duncan, Peter J.S. 2013. "Batman and Robin? Exploring foreign policy differences between Putin and Medvedev during the Medvedev presidency." Working paper 2013-03. UCL School of Slavonic and East European Studies, Centre for European Politics, Security & Integration. https://discovery.ucl.ac.uk/id/eprint/1400396/1/CEPSI-WP-2013-3-%20Duncan.pdf (accessed December 14, 2019)

Easterly, William and Stanly Fischer. 1994. *The Soviet Economic Decline: Historical and Republican Data* (Washington, DC: The World Bank).

eBay. 2019. "EBay Inc. Report Fourth Quarter and Full Year 2018 Results and Announces Capital Structure Evolution." https://www.ebayinc.com/stories/news/ebay-q4-2018-results/ (accessed April 29, 2019).

The Economist. 2020a. "Competition, sanctions and the new geopolitics of Russian gas." January 23. https://www.economist.com/finance-and-economics/2020/01/23/competition-sanctions-and-the-new-geopolitics-of-russian-gas (accessed February 26, 2020).

---. 2020b. "Memory Wipe." 434(9178): 42-43.

---. 2020c. "The search to find an alternative to the dollar: China, Russia and others don't want to rely on American high-finance." https://www.economist.com/leaders/2020/01/18/%20the-search-to-find-an-alternative-to-the-dollar (accessed January 23, 2020).

---. 2016. "Vladimir Putin's unshakable popularity: The Russian president's approval ratings refuse to budge." February 4. https://www.economist.com/graphic-detail/2016/02/04/vladimir-putins-unshakeable-popularity (accessed December 22, 2019).

---. 2011. "Russia's presidency: The Putin v Medvedev tandem." April 7th. https://www.economist.com/europe/2011/04/07/the-putin-v-medvedev-tandem (accessed December 14, 2019).

---. 2007. "Russia's booming economy: It's not about just oil and gas." June 18. https://www.economist.com/news/2007/06/18/russias-booming-economy (accessed December 07, 2019).

---. 2005. "Hurricane Katrina: The shaming of America." September 8. https://www.economist.com/leaders/%202005/09/08/the-shaming-of-america (accessed December 07, 2019).

Ennis, Stephen. 2014. "Dmitry Kiselyov: Russia's chief spin doctor." *BBC* 02 April. https://www.bbc.com/news/world-europe-26839216 (accessed January 12, 2020).

Electricity Information Sharing and Analysis Center (E-ISAC). 2016. *Analysis of the Cyber Attack on the Ukrainian Power Grid* (Washington, DC: E-ISAC).

Eriksson, Johan. 2007. “Power Disparity in the Digital Age.” In Olav F. Knudsen, Ed. *Security Strategies, Power Disparity and Identity: The Baltic Sea Region* (London: Routledge), 123-147.

Ermolaev, Sergei. 2017. “The Formation and Evolution of the Soviet Union’s Oil and Gas Dependence.” Carnegie Endowment for International Peace. https://carnegieendowment.org/2017/03/29/formation-and-evolution-of-soviet-union-s-oil-and-gas-dependence-pub-68443 (accessed July 25, 2019).

Estonian Atlantic Treaty Association. 2020. “NATO Member States.” https://www.eata.ee/en/nato-2/nato-member-states/ (accessed March 3, 2020).

Eun, Yong-Soo and Judith Sita Abmann. 2016. “Cyberwar: Taking Stock of Security and Warfare in the Digital Age.” *International Studies Perspectives* 17: 343-360.

Eurasian Economic Union (EEU). 2014. “Treaty on the Eurasian Economic Union.” http://www.eaeunion.org/?lang=en#info (accessed January 23, 2020).

European Court of Human Rights (ECHR). 2017. *Case of Tagayeva and Others v. Russia*. 13 April. https://hudoc.echr.coe.int/eng#_Toc478129552 (accessed December 22, 2019).

---. 2011. *Case of Finogenov and Others v. Russia*. 20 December. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-108231%22]} (accessed December 22, 2019).

European Union. 2019. “Shedding light on energy in the EU - A guided tour of energy statistics.” https://ec.europa.eu/eurostat/cache/infographs/energy/bloc-2c.html (accessed February 26, 2020).

---. 2017. *Russia’s national security strategy and military doctrine and their implications for the EU* (Belgium: EU Parliament).

Fakiolas, Efstathios T. 2003. “Continuity and Change in Soviet and Russian Grand Strategy.” *Mediterranean Quarterly* 9(2): 76-91.

Falliere, Nicolas, Liam O Murchu, and Eric Chien. 2011. *W32 Stuxnet Dossier, Version 1.4* (Symantec).

Farwell, James P. and Rafal Rohozinski. 2012. “The New Reality of Cyber War.” *Survival* 54(4), 107-120.

Fasanotti, Federica Saini. 2016. “Order from Chaos: Russia and Libya: A brief history of an on-again-off-again friendship.” Brookings. https://www.brookings.edu/blog/order-from-chaos/2016/09/01/russia-and-libya-a-brief-history-of-an-on-again-off-again-friendship/ (accessed March 7, 2020).

Feickert, Andrew and Stephen Daggett. 2012. *A Historical Perspective on “Hollow Forces”* (Washington, DC: Congressional Research Service).

Fidler, David P. 2012. “Tinker, Tailor, Soldier, Duqu: Why cyberespionage is more dangerous than you think.” *International Journal of Critical Infrastructure Protection* 5: 28–29

FIRST.org. 2015. “Common Vulnerability Scoring System v3.0: User Guide.” https://www.first.org/cvss/v3.0/cvss-v30-user_guide_v1.6.pdf (accessed May 14, 2019).

Fischer, Beth A. 2010. *"US foreign policy under Reagan and Bush." In* Leffler, Melvyn P. and Odd Arne Westad, Ed. 2010. *The Cambridge History of the Cold War, Vol III*. Cambridge: Cambridge University Press, 267-288.

Flournoy, Michéle and Michael Sulmeyer. 2018. "Battlefield Internet." *Foreign Affairs* 97(5): 40-46.

Fortune. 2019. "Fortune 500: The Top 10." https://fortune.com/fortune500/ (accessed April 16, 2019).

---. 1980. "Fortune 500: A database of 50 years of FORTUNE's list of America's largest corporations (1980 Full list)." https://archive.fortune.com/magazines/fortune/fortune500_archive/%20full/1980/ (accessed April 16, 2019).

Fox, Amos C. Major, U.S. Army. 2019. *"Cyborgs at Little Stalingrad": A Brief History of the Battles of the Donetsk Airport 26 May 2014 to 21 January 2015* (Arlington: Institute of Land Warfare).

Fox-Brewster, Thomas. "Petya Or NotPetya: Why The Latest Ransomware Is Deadlier Than WannaCry." *Forbes.* June 27. https://www.forbes.com/sites/thomasbrewster/2017/06/27/%20petya-notpetya-ransomware-is-more-powerful-than-wannacry/#dedfb7717417 (accessed April 21, 2019).

Fox, Susannah. 2014. *The Web at 25 in the U.S. Part 1: How the internet has woven itself into American Life* (Pew Research Center).

Freedman, Lawrence. 2017. *The Future of War: A History* (New York: Public Affairs).

Freiré, Maria Raquel. 2009. "Russian Policy in Central Asia: Supporting, Balancing, Coercing, or Imposing?" *Asian Perspective* 33(2): 125-149.

Fritze, John. 2017. "House committee releases Russian-linked ad depicting Freddie Gray." *The Baltimore Sun*. November 01. https://www.baltimoresun.com/politics/bs-md-russian-facebok-ad-20171101-story.html (accessed January 15, 2020)

Fukuyama, Francis. 1992. *The End of History and the Last Man* (New York: Free Press).

Gaddis, John Lewis. 2011. "9/11 in Retrospect: George W. Bush's Grand Strategy, Reconsidered." *Foreign Affairs* 90(5).

---. 2005a. *Strategies of Containment: A Critical Appraisal of American National Security Policy During the Cold War* (Oxford: Oxford University Press).

---. 2005b. "Grand Strategy in the Second Term." *Foreign Affairs* 84(1).

Gaddy, Clifford G. 2007. "The Russian Economy in the Year 2006." *Post-Soviet Affairs* 23: 38-49.

Garber, Megan. 2014. "The First Characters Sent Through the Internet Were L-O-L." *The Atlantic*, October 29. https://www.theatlantic.com/technology/archive/2014/10/the-first-characters-sent-through-the-internet-were-l-o-l/382074/ (accessed April 20, 2019).

Gartzke, Erik. 2013. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.” *International Security* 38 (Fall): 41–73.

Gat, Azar. 2018. *War and Strategy in the Modern World: From Blitzkrieg to Unconventional Terror* (London: Routledge).

George, Alexander L. and Andrew Bennett. 2004. *Case Studies and Theory Development in the Social Sciences* (Cambridge: MIT Press).

Gibbs, David. 1987. “Does the USSR Have a ‘Grand Strategy’? Reinterpreting the Invasion of Afghanistan.” *Journal of Peace Research* 24(4): 365-379.

Giles, Keir. 2016. “Russia’s ‘New’ Tools for Confronting the West: Continuity and Innovation in Moscow’s Exercise of Power.” Chatham House, The Royal Institute of International Affairs. https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf (accessed January 23, 2020).

Gilsinan, Kathy. 2019. “A Boom Time for U.S. Sanctions: The explosive growth in their use has prompted questions about how much is too much.” *The Atlantic* (May). https://www.theatlantic.com/politics/archive/2019/05/why-united-states-uses-sanctions-so-much/588625/ (accessed February 08, 2020).

Glantz, David M. 1991. *Soviet Military Operational Art: In Pursuit of Deep Battle* (Oxon: Frank Cass and Company).

Gleijeses, Piero. 2016. “The CIA’s paramilitary operations during the cold war: an assessment.” *Cold War History* 16(3): 291-306.

Gorbachev, Mikhail. 1988. “Address by Mikhail Gorbachev at the UN General Assembly Session (Excerpts)” The Cold War International History Project. https://digitalarchive.wilsoncenter.org/document/116224 (accessed Sep 22, 2019).

---. 1988. Foreign Relations – USSR. The Democratization of World Politics. Delivered to Yugoslavia’s Federal Assembly.” March 16. *Vital Speeches of the Day* 54(14): 418-421.

---. 1986. “Speech delivered at the Presentation of the Order of Lenin.” July 28. *Vital Speeches of the Day* 52(23): 706-711.

---. 1985a. “The Geneva Meeting: Domestic and Foreign Policies. Delivered at the Session of the U.S.S.R. Supreme Soviet.” November 27. *Vital Speeches of the Day* 52(7): 194-203.

---. 1985b. “Social and Economic Development.” *Vital Speeches of the Day* 51(13): 386-388.

Gordon, Phillip H. 2001. “Bush-Putin: The End of the End of the Cold War.” Brookings Institute. November 13. https://www.brookings.edu/opinions/bush-putin-the-end-of-the-end-of-the-cold-war/ (accessed February 17, 2020).

Götz, Elias. 2015. “It’s geopolitics, stupid: explaining Russia’s Ukraine policy.” *Global Affairs* 1(1): 3-10.

Goldman, Emily O. and Michael Warner. 2017. "Why a Digital Pearl Harbor Makes Sense . . . and Is Possible." In George Pekovich and Ariel E. Levite. *Understanding Cyber Conflict: 14 Analogies*, 147-157 (Washington, DC: Georgetown University Press).

Government Accountability Office (GAO). 2018. *Report to the Committee on Armed Services, U.S. Senate: Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities* (Washington, DC: GAO).

---. 2017a. *Cybersecurity: Federal Efforts Are Under Way that May Address Workforce Challenges.* Testimony Before the Subcommittee on Information Technology, Committee on Oversight and Government Reform, House of Representatives (Washington, DC: GAO).

---. 2017b. *Overseas Contingency Operations: OMB and DOD Should Revise Criteria for Determining Eligible Costs and Identify the Costs Likely to Endure Long Term* (Washington, DC: GAO).

---. 2016. *Testimony Before the Committee on Oversight and Government Reform, House of Representatives: Information Technology: Federal Agencies Need to Address Aging Legacy Systems*. May 25 (Washington, DC: GAO) https://www.gao.gov/assets/680/677454.pdf (accessed May 2, 2019).

---. 2013. *Financial Regulatory Reform: Financial Crisis Losses and Potential Impacts of the Dodd-Frank Act* (Washington, DC: GAO).

Graff, Garrett M. 2017a. "A Guide to Russia's High Tech Tool Box for Subverting US Democracy." *Wired.* August 13. https://www.wired.com/story/a-guide-to-russias-high-tech-tool-box-for-subverting-us-democracy/ (accessed January 18, 2020).

---. 2017b. "How a Dorm Room *Minecraft* Scam Brought Down the Internet." *Wired* December 13. https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/ (accessed May 16, 2019).

Grant, Rebecca. 2016. "The Second Offset." *Air Force Magazine* (July): 32-36.

Greathouse, Craig B. 2010. "Examining the Role and Methodology of Strategic Culture." *Risk, Hazards & Crisis in Public Policy* 1(1): 57-85.

Greenberg, Andy. 2020. "If Russia Hacked Burisma, Brace for the Leaks to Follow." *Wired* January 14. https://www.wired.com/story/russia-burisma-hack-leaks/ (accessed January 24, 2020).

---. 2019. "How Not To Prevent a Cyberwar With Russia: Former cybersecurity officials warn against a path of aggression that could inflame cyberwar rather than deter it." *Wired* June 10. https://www.wired.com/story/russia-cyberwar-escalation-power-grid/ (accessed April 1, 2020).

---. 2017. "How an Entire Nation Became Russia's Test Lab for Cyberwar." Wired June 20. https://www.wired.com/story/russian-hackers-attack-ukraine/ (accessed April 29, 2019).

Grigas, Agnia. 2012. "Legacies, Coercion and Soft Power: Russian Influence in the Baltic States." Chatham House, The Royal Institute of International Affairs. August 1. https://www.chathamhouse.org/publications/papers/view/185321 (accessed April 2, 2020).

Grimes, Roger A. 2016. "Why it's so hard to prosecute cyber criminals." December 6. https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html (accessed May 9, 2019).

Gromyko, Andrei. 1983. "The International Situation: The Foreign Policy of the Soviet Union. Delivered at the Eighth Session of the Supreme Soviet of the U.S.S.R." June 16. *Vital Speeches of the Day* 49(19): 578-586.

---. 1981. "How to Preserve Peace, delivered at the 36th Session of the United Nations General Assembly." September 22. *Vital Speeches of the Day* 48(5): 130-137.

Grossman, Erik J. 2018. "Russia's Frozen Conflicts and the Donbas." *Parameters* 48(2): 51-61.

The Guardian. 2012. "Putin: we won Russian election honestly and fairly – video." https://www.theguardian.com/world/video/2012/mar/05/putin-we-won-russian-election-video (accessed December 20, 2019).

Gurganus, Julia. 2018. "How (and Why) Russia Does More with Less." In John R. Deni, Ed. *Current Russia Military Affairs: Assessing and Counter Russian Strategy, Operational Planning, and Modernization* (Carlisle: Strategic Studies Institute), 10-13.

Haas, Marcel de. 2011. *Clingendael Paper No. 5. Russia's Military Reforms: Victory after Twenty Years of Failure?* (The Hague: Netherlands Institute of International Relations "Clingendael").

Haddad, Benjamin and Alina Polyakova. 2018. "Don't rehabilitate Obama on Russia." The Brookings Institution. March 5. https://www.brookings.edu/blog/order-from-chaos/2018/03/05/dont-rehabilitate-obama-on-russia/ (accessed February 19, 2020).

Hanson, Phillip. 1986. "Soviet foreign trade and Europe in the late 1980s." *The World Today* 42(8/9): 144-146.

Harris, Brice F. 2014. "United States Strategic Culture and Asia-Pacific Security." *Contemporary Security Policy* 32(2): 290-309.

Harrison, Todd. "What Has the Budge Control Act of 2011 Meant for Defense?" Center for Strategic and International Studies. August 1. https://www.csis.org/analysis/what-has-budget-control-act-2011-meant-defense (accessed December 15, 2019).

Hathaway, Melissa. 2017. *CIGI Papers No. 127: Getting beyond Norms When Violating the Agreement Becomes Customary Practice.* Waterloo: Center for International Governance Innovation. https://www.cigionline.org/sites/default/files/documents/Paper%20no.127.pdf (accessed March 15, 2019).

He, Kai. 2017. "Explaining United States – China relations: neoclassical realism and the nexus of threat – interest perceptions." *The Pacific Review* 30(2): 133-151.

Heitman, Sydney. 1991. "Soviet emigration in 1990: A new 'fourth wave'?" *Innovation in Social Sciences Research* 4(3/4): 1-15.

Helliwell, John F. "Comparative Macroeconomics of Stagflation." *Journal of Economic Literature* 26(March): 1-28.

Hemmer, Christopher. 2015. *American Pendulum: Recurring Debates in U.S. Grand Strategy* (Ithaca: Cornell University Press).

Henry-Nickie, Makada, Kwadwo Frimpong, and Hao Sun. 2019. "Trends in the Information Technology Sector." Brookings. March 29. https://www.brookings.edu/research/trends-in-the-information-technology-sector/ (accessed March 22, 2020).

Herspring, Dale R. 2009. "Vladimir Putin: His Continuing Legacy." *Social Research* 76(1): 151-174.

Hoffman, Frank G. 2018. "Exploring War's Character & Nature. Will War's Nature Change in the Seventh Military Revolution?" *Parameters* 47(4): 19-31.

Human Rights Watch. 2019. "World Report 2019: Our annual review of human rights around the globe." https://www.hrw.org/world-report/2019 (accessed December 20, 2019).

IDC. 2019. "IDC Forecasts Revenues for Big Data and Business Analytics Solutions Will Reach $189.1 Billion This Year with Double-Digit Annual Growth Through 2022." April 04. https://www.idc.com/getdoc.jsp?containerId=prUS44998419 (Accessed April 30, 2019).

Ibarra-Esquer, Jorge E., Felix F. Gonzalez-Navarrow, Brenda L. Flores-Rios, Larysa Burtseva, and Maria A. Astorga-Vargas. 2017. "Tracking the Evolution of the Internet of Things Concept Across Different Application Domains." *Sensors* 17(1370): 1-24.

IHS Markit. 2019. "Islamic State Territory Down 60 Percent and Revenue Down 80 Percent on Caliphate's Third Anniversary, IHS Markit Says." http://news.ihsmarkit.com/prviewer/release_%20only/%20slug/aerospace-defense-security-islamic-state-territory-down-60-percent-and-revenue-down-80 (accessed December 15, 2019).

Ikenberry, G. John, Michael Mastanduno and William C. Wohlforth. 2011. *International Relations Theory and the Consequences of Unipolarity* (Cambridge: Cambridge University Press).

Inkster, Nigel. 2018. "Why we need to measure military cyber power." March 29. https://www.weforum.org/ (accessed May 17, 2019).

Intelligence and National Security Alliance (INSA). 2018. "Managing A Cyber Attack On Critical Infrastructure: Challenges of Federal, State, Local, and Private Sector Collaboration." https://www.insaonline.org/wp-content/uploads/2018/08/INSA-Managing-Cyber-Attack-Critical-Infrastructure.pdf (accessed May 15, 2019).

Interfax. 2018. "The State Duma approved a draft document on the revision of political assessments of the war in Afghanistan." November 21. https://www.interfax.ru/russia/638844 (accessed March 7, 2020).

International Monetary Fund (IMF), International Bank for Reconstruction and Development / The World Bank; Organisation for Economic Co-operation and Development; and European

Bank for Reconstruction and Development. 1990. *The Economy of the USSR* (Washington, DC: The World Bank).

Ioffe, Julia. “The History of Russian Involvement in America’s Race Wars: From propaganda posters to Facebook ads, 80-plus years of Russian meddling.” *The Atlantic* 21 October. https://www.theatlantic.com/international/archive/2017/10/russia-facebook-race/542796/ (accessed January 15, 2020).

Itani, Faysal. 2017. “The End of American Support for Syrian Rebels Was Inevitable.” *The Atlantic*. July 21. https://www.theatlantic.com/international/archive/2017/07/trump-syria-assad-rebels-putin-cia/534540/ (accessed March 7, 2020)

Jacques, Martin. 2009. *When China rules the world: the rise of the middle kingdom and the end of the Western world* (London: Penguin).

Jenkins, Brian. 2013. “Keeping up with Zuck: A Brief History of Facebook Features.” *Techniques* November/December: 60-61.

Kahn, Herman. 1960. *On Thermonuclear War* (London: Routledge).

Kallas, Kristina. 2016. “Claiming the diaspora: Russia’s compatriot policy and its reception by Estonian-Russian population.” *Journal on Ethnopolitics and Minority Issues in Europe* 15(3): 1-25.

Kara-Murza, Vladimir. 2018. “Defying history, Moscow moves to defend Soviet war in Afghanistan.” *The Washington Post*. December 4. https://www.washingtonpost.com/opinions/%202018/12/04/defying-history-moscow-moves-defend-soviet-war-afghanistan/ (accessed March 7, 2020).

Kasapoglu, Can. 2015. *Russia’s Renewed Military Thinking: Non-Linear Warfare and Reflexive Control* (Rome: NATO Defense College).

Katzenstein, Peter J., ed. 1996. *The Culture of National Security: Norms and Identity in World Politics* (New York: Columbia University Press).

Keenan, George F. 1947. “The Sources of Soviet Conduct.” *Foreign Affairs* (July).

Kello, Lucas. 2017. *The Virtual Weapon and International Order* (New Haven: Yale University Press).

---. 2013. “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft.” *International Security* 38 (Fall): 7-40.

Kemp, Simon. 2019. *Digital 2019: Global Digital Yearbook* (Singapore: Kepios). https://datareportal.com/reports/digital-2019-global-digital-yearbook?utm_source=Reports&utm_medium=PDF&utm_campaign=Digital_2019&utm_content=Global_Overview_Promo_Slide (accessed April 11, 2019).

KGB. 1985. Douglas Selvage, trans. “Information Nr. 2955 [to Bulgarian State Security]." September 07. History and Public Policy Program Digital Archive, Committee for Disclosing the Documents and Announcing the Affiliation of Bulgarian Citizens to the State Security and the

Intelligence Services of the Bulgarian National Army (CDDAABCSSISBNA-R). Obtained by https://digitalarchive.wilsoncenter.org/document/208946 (accessed September 21, 2019).

King, Gary, Robert O. Keohane, and Sidney Verba. 1994. *Designing Social Inquiry: Scientific Inference in Qualitative Research* (Princeton: Princeton University Press).

Kingsbury, Alex. 2009. "Declassified Documents Reveal KGB Spies in the U.S." *U.S. News & World Report* July 17. https://www.usnews.com/news/articles/2009/07/17/declassified-documents-reveal-kgb-spies-in-the-us (accessed October 06, 2019).

Kintner, William R. 1987. *Soviet Global* Strategy (Fairfax: Hero Books).

Kitchen, Nicholas. 2010. "Systemic pressures and domestic ideas: a neoclassical realist model of grand strategy formation." *Review of International Studies* 38: 117-143.

Klein, Margarete. 2015. "Russia's New Military Doctrine: NATO, the United States and the "Colour Revolutions." *SWP Comments* 9: 1-4.

Kleveman, Lutz. 2003. *The New Great Game: Blood and Oil in Central Asia* (New York: Atlantic Monthly Press).

Kochetkova, Elena, David Damtas, Lilia Boliachevets, Polina Slyusarchuk, and Julia Lajus. 2017. "Soviet Technological Projects and Technological Aid in Africa and Cuba, 1960s-1980s." Basic Research Paper, National Research University Higher School of Economics.

Kofman, Michael. 2018. "The role of Pre-conflict Conflict and the Importance of the Syrian Crucible." In John R. Deni, Ed. *Current Russia Military Affairs: Assessing and Counter Russian Strategy, Operational Planning, and Modernization* (Carlisle: Strategic Studies Institute), 21-24.

Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer. 2017. *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Monica: RAND).

Kokoshin, Andrei. 1999. *Soviet Military Thought: 1917-1991* (Cambridge: The MIT Press).

Kotkin, Stephen. 2016. "Russia's Perpetual Geopolitics: Putin Returns to the Historical Pattern." *Foreign Affairs* 95(3): 2-9.

---. 2018. "Realist World: The Players Change, but the Game Remains." *Foreign Affairs* 97(4): 10-15.

Kolstø, Pål. 2016. "Crimea vs. Donbas: How Putin Won Russian Nationalist Support – and Lost it Again." *Slavic Review* 75(3): 702-725.

Kotkin, Stephen. 2016. "Russia's Perpetual Geopolitics: Putin Returns to the Historical Pattern." *Foreign Affairs* 95(3): 2-9.

Kozhanov, Nikolay. 2016. "Arms Exports Add to Russia's Tools of Influence in Middle East." Chatham House, The Royal Institute of International Affairs. July 20. https://www.chathamhouse.org/expert/comment/arms-exports-add-russia-s-tools-influence-middle-east (accessed January 25, 2020).

Kremlin. 2019a. “Belt and Road Forum for International Cooperation.” http://en.kremlin.ru/%20events/president/news/60378 (accessed January 24, 2020).

---. 2019b. “Conference on artificial intelligence.” http://en.kremlin.ru/events/%20president/news/62003 (accessed January 21, 2020).

---. 2019c. “Direct line with Vladimir Putin.” http://en.kremlin.ru/events/president/news/60795 (accessed January 25, 2020).

---. 2019d. “Meeting with representatives of Russian news agencies and print media.” http://en.kremlin.ru/events/president/news/59865 (accessed January 20, 2020).

---. 2019e. “Plenary session of the International Arctic Forum.” http://en.kremlin.ru/%20events/president/news/60250 (accessed January 25, 2020).

---. 2019f. “Presidential Address to Federal Assembly.” http://en.kremlin.ru/events/%20president/news/59863 (accessed January 21, 2020).

---. 2019g. “Press statements following Russian – Chinese talks.” http://en.kremlin.ru/events/%20president/news/60672 (accessed January 24, 2020).

---. 2019h. “Talks with President of Venezuela Nicolas Maduro.” http://en.kremlin.ru/%20events/president/news/61640 (accessed March 30, 2020).

---. 2017a. “Meeting on Arctic region’s comprehensive development.” http://en.kremlin.ru 20events/president/news/54147 (accessed January 25, 2020).

---. 2017b. “Meeting with founder of Ethereum project Vitalik Buterin.” http://en.kremlin.ru/%20events/president/news/54677 (accessed January 25, 2020)

---. 2016. “Meeting of the Valdai International Discussion Club.” http://en.kremlin.ru/%20events/president/news/53151 (accessed March 31, 2020).

---. 2015. “70th session of the UN General Assembly.” http://en.kremlin.ru/events/%20president/news/50385 (accessed January 24, 2020).

---. 2014. “Meeting of the Valdai International Club.” http://en.kremlin.ru/events/president%20/news/46860 (accessed January 22, 2020).

---. 2007. “President Vladimir Putin congratulated the members of the Russian scientific research expedition to the North Pole.” http://en.kremlin.ru/events/president/%20news/41543 (accessed January 21, 2020).

Kuchins, Andrew C. 2015. “Mismatched Partners: US-Russia Relations after the Cold War.” In David Cadier and Margot Light, Ed. *Russia’s Foreign Policy: Ideas, Domestic Politics and External Relations* (New York: Palgrave MacMillan), 117-137.

Kumar, Nallapaneni Manoj and Pradeep Kumar Mallick. 2018. “The Internet of Things: Insights into the building blocks, component interactions, and architecture layers.” *Procedia Computer Science* 132: 109-117.

LaGrone, Sam. 2019. “U.S. 2nd Fleet Declares Operational Capability Ahead of Major European Exercise.” *United States Naval Institute News*. May 29. https://news.usni.org/2019/05/29/u-s-2nd-fleet-declares-operational-capability-ahead-of-major-european-exercise (accessed February 22, 2020).

Lankina, Tomila and Kohei Watanabe. 2017. “’Russia Spring’ or ‘Spring Betrayal’? The Media as a Mirror of Putin’s Evolving Strategy in Ukraine.” *Europe-Asia Studies* 69(10): 1526-1556.

Lantis, Jeffrey S. 2014. “Strategic Cultures and Security Policies in the Asia-Pacific.” *Contemporary Security Policy* 35(2): 166-186.

Lavrov, Sergey. 2014. “Speech by the Russian Foreign Minister, Sergey Lavrov, at the 50th Munich Security Conference, Munich, 1 February 2014.” http://www.rusembdprk.ru/en/press-releases/106-speech-by-the-russian-foreign-minister-sergey-lavrov-at-the-50th-munich-security-conference-munich-1-february-2014 (accessed January 20, 2020).

Leake, Elizabeth. 2018. “Spooks, Tribes, and Holy Men: The Central Intelligence Agency and the Soviet Invasion of Afghanistan.” *Journal of Contemporary History* 53(1): 240-262.

Leffler, Melvyn P. and Odd Arne Westad, Ed. 2010. *The Cambridge History of the Cold War, Vols I – III* (Cambridge: Cambridge University Press).

Leiner, Barry M., Robert E. Kahn, Jon Postel, Vinton G. Cerf, Leonard Kleinrock, Larry G. Roberts, David D. Clark, Daniel C. Lynch, Stephen Wolff. 2009. “A Brief History of the Internet.” *ACM SIGCOMM Computer Communication Review* 39(5): 22-31.

Lenta.ru. 2014. “Volodin identified Russia and Putin.” 22 October. https://lenta.ru/news/2014%20/10/22/%20waldai/ (translated by DeepL.com; accessed December 14, 2019).

Levick, Ewen. 2018. “Russia: patrons of assassinations.” 18 May. Lowy Institute. https://www.lowyinstitute.org/%20the-interpreter/russia-patrons-assassinations (accessed 12 January 2020).

Lewis, James. “Economic Impact of Cybercrime – No Slowing Down.” February. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_%202018_02_21&utm_medium=email (accessed May 16, 2019).

Li, Mia Shuang. 2018. “How WeChat became the primary news source in China.” *Columbia Journalism Review* January 10. https://www.cjr.org/tow_center/how-wechat-became-primary-news-source-china.php (accessed May 1, 2019).

Libicki, Martin C. 2011. “The Nature of Strategic Instability in Cyberspace.” *Brown Journal of World Affairs* 18 (Fall/Winter) 2011: 71-79

Lieber, Robert J. 2016. *Retreat and Its Consequences: American Foreign Policy and the Problem of the World Order* (New York: Cambridge University Press).

Liff, Adam P. 2012. “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare capabilities and Interstate War.” *The Journal of Strategic Studies* 35 (June): 401–428.

Light, Margot. 2008. “Russian-American Relations under George W. Bush and Vladimir Putin.” *Irish Studies in International Affairs* 19: 25-32.

Lindsay, Joh R. and Tai Ming Cheung. 2015. “From Exploitation to Innovation: Acquisition, Absorption and Application.” In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain,e*ds. Lindsay, Jon R., Tai Ming Cheung and Derek S. Reveron (New York: Oxford University Press).

Lipman, Maria. “How Putin Silences Dissent: Inside the Kremlin’s Crackdown.” *Foreign Affairs* 95(3): 38-46.

Lo, Bobo. 2017. “An Accident Waiting to Happen: Trump, Putin and the US-Russia Relationship.” Lowy Institute. October 25. https://www.lowyinstitute.org/publications/accident-waiting-happen-trump-putin-and-us-russia-relationship (accessed February 18, 2020).

Lomagin, Nikita A. 2007. “Forming a New Security Identity Under Vladimir Putin.” In Kanet, Roger E. Ed. *Russia: Reemerging Great Power* (New York: Palgrave MacMillan), 31-53.

Lopez, Todd C. 2019. “Losing Technology to Competitors Threatens Force Lethality.” October 31. https://www.defense.gov/Explore/News/Article/Article/2004140/losing-technology-to-competitors-threatens-force-lethality/ (accessed March 1, 2020).

Lueth, Knud Lasse. 2018. “State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating.” IOT Analytics Gmbh. https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/ (accessed April 16, 2019).

Lukasik, Stephen J. 2011. “Why the Arpanet Was Built.” *IEEE Annals of the History of Computing* July-August: 4-20.

Lukyanov, Fyodor. 2016. “Putin’s Foreign Policy: The Quest to Restore Russia’s Rightful Place.” *Foreign Affairs* 95(3): 30-37.

Luttwak, Edward N. 1983. *The Grand Strategy of the Soviet* Union (New York: St. Martin’s Press).

Luxmoore, Matthew. 2019. “How a Local Vote Rocked Russia: Moscow Election Caps Summer of Discontent.” Radio Free Europe / Radio Liberty. September 6. https://www.rferl.org/a/how-a-local-vote-rocked-russia-moscow-election-caps-summer-of-discontent/30150471.html (accessed December 20, 2019).

Macrotrends LLC. 2019. “Market Capitalization.” www.macrotrends.net (accessed April 16, 2019).

Malik, Rohit, Sandeep Dalal, and Kamna Solanki. 2018. “Literature Review on Security Aspects of IOT.” *International Journal of Advanced Research in Computer Science* 9(2): 123-126.

Martel, William C. *Grand Strategy in Theory and Practice: The Need for an Effective American Foreign Policy* (Cambridge: Cambridge University Press).

Marten, Kimberly. 2019. “Russia’s use of semi-state security forces: the case of the Wagner Group.” *Post-Soviet Affairs* 35(3): 181-204.

Masters, Jonathan. 2019. “The North Atlantic Treaty Organization (NATO).” Council on Foreign Relations. December 3. https://www.cfr.org/backgrounder/north-atlantic-treaty-organization-nato (accessed November 30, 2019).

Mavadiya, Madhvi. 2017. “Putin And Ethereum: A Match Made In Fintech.” *Forbes*. August 29. https://www.forbes.com/sites/madhvimavadiya/2017/08/29/putin-ethereum-fintech/#7b1815556b5c (accessed January 25, 2020).

MccGwire, Michael. 1992. *Perestroika and Soviet National Security* (Washington, DC: Brookings Institute).

McChrystal, Stanley, General, US Army, retired. 2015. *Team of Teams: New Rules of Engagement for a Complex World* (New York: Portfolio Penguin).

McClory, Jonathan. 2018. *The Soft Power 30: A Global Ranking of Soft Power 2018* (Singapore: Portland).

McQuade, Mike. 2018. “The Untold Story of NotPetya, the Most Devastating Cyberattack in History.” *Wired.* August 22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (accessed January 18, 2020).

McGraw, Gary. 2013. “Cyber War is Inevitable (Unless We Build Security In).” *Journal of Security Studies*. 36 (1): 109-119.

Mearsheimer, John. 2001. *The Tragedy of Great Power Politics* (New York: W.W. Norton & Company, Inc.).

---. 1982. “Why the Soviets Can’t Win Quickly in Central Europe.” *International Security* 7(1): 3-39.

Mee, Paul and Til Schuermann. 2018. “How a Cyber Attack Could Cause the Next Financial Crisis” *Harvard Business Review* (September 14). https://hbr.org/2018/09/how-a-cyber-attack-could-cause-the-next-financial-crisis (accessed May 16, 2019).

Meese, Edwin III. 1992. “The Man Who Won the Cold War.” *Policy Review* 61: 36-40.

Mehta, Aaron. 2020. “Trump’s new nuclear weapon has been deployed.” *Defense News*. February 4. https://www.defensenews.com/smr/nuclear-arsenal/2020/02/04/trumps-new-nuclear-weapon-has-been-deployed/ (accessed February 22, 2020).

Mikkola, Harri. 2019. *Briefing Paper 259. The Geostrategic Arctic: Hard Security in the High North* (Helsinki: Finnish Institute of International Affairs).

Miller, Chris. 2018. “The Surprising Success of Putinomics: Behind Putin’s Formula for Holding Onto Power.” *Foreign Affairs*. February 7. https://www.foreignaffairs.com/articles/russian-federation/2018-02-07/surprising-success-putinomics (accessed January 18, 2020).

Minakov, Mykhailo. 2018. “The Significance of the Euromaidan for Ukraine and Europe.” The Wilson Center. November 21. https://www.wilsoncenter.org/blog-post/the-significance-euromaidan-for-ukraine-and-europe (accessed December 20, 2019).

Milevski, Lukas. 2016. “The Nature of Strategy Versus the Character of War.” *Comparative Strategy* 35(5): 438-446.

Ministry for State Security (STASI). 1983. Bernd Schaefer trans. “Notes on Statements Made by Comrade Colonel General Kryuchkov.” October 03 https://digitalarchive.wilsoncenter.org/document/119321 (accessed September 21, 2019).

Ministry of Foreign Affairs of Japan. 2017. “Japan-Russia Foreign and Defence Ministerial Consultation (‘2+2’ Ministerial Meeting).” https://www.mofa.go.jp/erp/rss/northern/%20page4e_000593.html (accessed January 22, 2020).

Miyoshi, Osamu. 1987. “Soviet Collective Security Pacts.” In Cline, Ray, James Arnold Miller, and Roger E. Kanet, Eds. *Asia in Soviet Global Strategy* (Boulder: Westview Press), 23-32.

Monaghan, Andrew. 2011. “The Russian Vertikal: the Tandem, Power, and the Elections.” Chatham House Russia and Eurasia Programme Paper REP 2011/01. Chatham House, The Royal Institute of International Affairs. https://www.chathamhouse.org/sites/default/files/%2019412_0511 ppmonaghan.pdf (accessed December 14, 2019).

Muro, Mark, Robert Maxim, and Jacob Whiton. 2019. *Automation and Artificial Intelligence: How machines are affecting people and places* (Washington, DC: Brookings Institution).

Murphy, Julia and Max Roser. 2019. “Internet.” https://ourworldindata.org/internet (accessed April 11, 2019).

Murray, Alan T. and Tony H. Grubesic, Ed. 2007. *Critical Infrastructure: Reliability and Vulnerability* (Berlin: Springer).

NASDAQ. 2019. “3 FAANG Stocks Rising in 2019. https://www.nasdaq.com/articles/3-faang-stocks-rising-in-2019-2019-03-07 (accessed April 29, 2019).

Nation, Craig R. 2012. “Reset or rerun? Sources of discord in Russian – American relations.” *Communist and Post-Communist Studies* 45: 379-387.

National Bureau of Asian Research. 2017. *The Report of the Commission on the Theft of American Intellectual Property* (Seattle: National Bureau of Asian Research).

National Cybersecurity Communications and Integration Center (NCCIC). 2016. “ICS-CERT Annual Assessment Report: Industrial Control Systems Cyber Emergency Response Team.” https://www.us-cert.gov/sites/default/files/Annual_Reports/FY2016_Industrial_%20Control_Systems_Assessment_Summary_Report_S508C.pdf (accessed May 15, 2019).

National Institute of Technology (NIST). 2019a. “CVSS Severity Distribution Over Time.” https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time (accessed May 14, 2019).

---. 2019b. “National Vulnerability Database: General Information.” https://nvd.nist.gov/general (accessed May 14, 2019).

National Security Telecommunications Advisory Committee (NSTAC). 2018. *NSTAC Report to the President on a Cybersecurity Moonshot* (Washington, DC: NSTAC).

Naughton, John. 2016. "The Evolution of the Internet: from Military experiment to General Purpose Technology." *Journal of Cyber Policy* 1 (1): 5-28.

---. 2000. *A Brief History of the Future: From Radio Days to Internet Years in a Lifetime* (Woodstock: The Overlook Press).

Nicoll, Alexander and Jessica Delaney. 2015. "Russian air patrols: long-range ambitions." *Strategic Comments* 21(4): iv-v.

North Atlantic Treaty Organization (NATO). 2020. "Enlargement" https://www.nato.int/%20cps/en/natolive/topics_49212.htm (accessed March 3, 2020).

---. 2019a. "Enlargement." https://www.nato.int/cps/en/%20natolive/topics_49212.htm (accessed December 5, 2019).

---. 2019b. "Statement to the Press by NATO Secretary General Jens Stoltenberg after meeting with US President Trump." November 14. https://www.nato.int/cps/en/natohq/opinions_%20170788.htm?selectedLocale=en (accessed April 2, 2020).

---. 2016. "Remarks by NATO Secretary General Jens Stoltenberg at the European Parliament Committee on Foreign Affairs and its Subcommittee on Security and Defence." https://www.nato.int/cps/en/natohq/opinions_128311.htm%3FselectedLocale%3Den (accessed January 25, 2020).

---. 1987. "Defence of Northern and Central Regions (In Place and Rapidly Deployable Forces)." https://www.nato.int/cps/fr/natohq/declassified_138256.htm (accessed September 29, 2019).

---. 1987. "Geostrategic Dissimilarities Between East and West." https://www.nato.int/cps/fr/natohq/declassified_138256.htm (accessed September 29, 2019).

Norwegian Intelligence Service. 2019. *Focus 2019*. https://forsvaret.no/fakta_/ForsvaretDocuments/focus2019_english_web.pdf (accessed January 12, 2020).

Norwood, Paul R., Benjamin M. Jensen, and Justin Barnes. 2016. "War: Theory and Practice: Capturing the Character of Future War." *Parameters* 46(2): 81-91.

Nuclear Threat Initiative. 2019. "Russia: Nuclear." https://www.nti.org/learn/countries/russia/nuclear/ (accessed January 12, 2020).

Nuechterlein, Donald E. 1990. "The Reagan Doctrine in Perspective." *Perspectives on Political Science* 90(19): 43-49.

Nye, David. 2015. "11 Spies Who did the Worst Damage to the U.S. Military." *Real Clear Defense* June 03. https://www.realcleardefense.com/articles/2015/06/04/11_%20american_spies_who_did_the_worst_damage_to_the_us_military_108022.html (accessed September 29, 2019).

---. 2011. *The Future of Power* (NY: Public Affairs).

Nye, Joseph. 2019. “Protecting Democracy in an Era of Cyber Information War.” Belfer Center for Science and International Affairs November 13. https://www.belfercenter.org/sites/default/files/files/publication/ProtectingDemocracy.pdf (accessed April 1, 2020).

Obar, Jonathan and Steve Wildman. 2015. “Social media definition and the governance challenge: An introduction to the special issue.” *Telecommunications Policy* 39: 745-750.

Office of Naval Intelligence. 2015. *The Russian Navy: An Historic Transition* (Washington, DC: ONI).

Office of Personnel Management (OPM). 2018. *Sizing Up the Executive Branch: Fiscal Year 2017* (Washington, DC: OPM). https://www.opm.gov/policy-data-oversight/data-analysis-documentation/federal-employment-reports/reports-publications/sizing-up-the-executive-branch-2016.pdf (accessed May 2, 2019).

Oliker, Olga. 2015. “Russia’s New Military Doctrine: Same as the Old Doctrine, Mostly.” The RAND Blog. https://www.rand.org/blog/2015/01/russias-new-military-doctrine-same-as-the-old-doctrine.html (accessed January 22, 2020).

Organization for Economic Cooperation and Development (OECD). 2018. “Gross domestic spending on R&D.” https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm (accessed March 21, 2020).

---. 2014. *The Space Economy at a Glance 2014* (Paris: OECD). https://read.oecd-ilibrary.org/economics/the-space-economy-at-a-glance-2014_9789264217294-en#page1 (accessed March 21, 2020).

---. 2006. *Information and Communications Technologies: OECD Information and Technology Outlook* (Paris: OECD).

Organization of the Treaty of Collective Security. 2020. http://www.odkb.gov.ru/start/index_aengl.htm (accessed January 23, 2020).

Østensen, Åse Gilje and Tor Bukkvoll. 2018. *Russian Use of Private Military and Security Companies – the implications for European and Norwegian Security* (Bergen: Norwegian Defence Research Establishment).

Patrikarakos, David. 2017. *War in 140 Characters: How Social Media Is Reshaping Conflict in the Twenty-First Century* (New York: Basic Books).

Peng Guanqian, Zhao Zhiyin, and Luo Yong. 2010. *China’s National Defense.* Trans. Ma Chenguang and Yan Shuang (Beijing: China Broadcasting Press).

Perrin, Andrew. 2017. “10 facts about smartphones as the iPhone turns 10.” https://www.pewresearch.org/fact-tank/2017/06/28/10-facts-about-smartphones/ (accessed May 1, 2019).

Persson, Emil and Bo Petersson. 2014. “Political mythmaking and the 2014 Winter Olympics in Sochi: Olympism and the Russian great power myth.” *East European Politics* 30(2): 192-209.

Pew Research Center. 2018a. “Digital News Fact Sheet.” https://www.journalism.org/fact-sheet/digital-news/ (accessed May 1, 2019).

---. 2018b. “Internet, social media use and device ownership in the U.S. have plateaued after years of growth.” https://www.pewresearch.org/fact-tank/2018/09/28/internet-social-media-use-and-device-ownership-in-u-s-have-plateaued-after-years-of-growth/ (accessed May 1, 2019).

---. 2017. “A third of Americans live in a household with three or more smartphones.” https://www.pewresearch.org/fact-tank/2017/05/25/a-third-of-americans-live-in-a-household-with-three-or-more-smartphones/ (accessed April 12, 2019)

Pigman, Lincoln. 2019. “Russia’s Compatriots: Instruments or Responsibility?” *The RUSI Journal* 164(2): 24-35.

Pinto, Alejandro. 2019. “Exploring Blockchain as the foundation for next gen apps on Web 3.0.” IBM, March 18. https://www.ibm.com/blogs/blockchain/2019/03/exploring-blockchain-as-the-foundation-for-next-gen-apps-on-web-3-0/ (accessed April 12, 2019).

Poell, Jeroen de Kloet and Guohua Zeng. 2014. “Will the real Weibo please stand up? Chinese online contention and actor-network theory.” *Chinese Journal of Communication* 7(1) 1-18.

Polyakova, Alina. 2019. “Testimony before the United States House Committee on Appropriations – Subcommittee on State, Foreign Operations, and Related Programs: United States Efforts to Counter Russian Disinformation and Malign Influence.” Brookings. July 10. https://www.brookings.edu/wp-content/uploads/2019/07/Alina-Polyakova-House-Appropriations-Testimony-July-10-2019.pdf (accessed March 15, 2020).

---. 2018. “Weapons of the weak: Russia and AI-driven asymmetric warfare.” The Brookings Institution. November 15. https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/ (accessed January 21, 2020).

Popescu, Nicu. 2018. “Russian cyber sins and storms.” European Council on Foreign Relations. 10 October. https://www.ecfr.eu/article/%20commentary_russian_cyber_sins_and_storms (accessed January 20, 2020).

Posen, Barry R. 2018. “The Rise of Illiberal Hegemony: Trump’s Surprising Grand Strategy,” *Foreign Affairs* (March/April 2018) https://www.foreignaffairs.com/articles/2018-02-13/rise-illiberal-hegemony (accessed February 8, 2020).

---. 2013. “Pull Back: The Case for a Less Activist Foreign Policy.” *Foreign Affairs* 92(1): 116-128.

Poushter, Jacob, Caldwell Bishop, and Hanuyu Chwe. 2018. “Social Media Use Continues to Rise in Developing Countries but Plateaus Across Developed Ones.” (Pew Research Center) https://www.pewresearch.org/global/2018/06/19/3-social-network-adoption-varies-widely-by-country/ (accessed May 1, 2019).

Putin, Vladimir. 2015. “70th session of the UN General Assembly.” http://en.kremlin.ru/events/%20president/%20news/50385 (accessed January 19, 2020).

---. 2013. “Opinion: A Plea For Caution from Russia.” *New York Times.* September 11. https://www.nytimes.com/2013/09/12/opinion/putin-plea-for-caution-from-russia-on-syria.html?_r=0 (accessed January 22, 2020).

---. 2007. “Speech and the Following Discussion at the Munich Conference on Security and Policy.” February 10. http://en.kremlin.ru/events/president/transcripts/24034 (accessed December 22, 2019).

---. 2005. “Annual Address to the Federal Assembly of the Russian Federation.” April 25. http://en.kremlin.ru/events/president/transcripts/22931 (accessed December 21, 2019).

Radford, Jynnah and Luis Noe-Bustamante. 2019. “Facts on U.S. Immigrants, 2017: Statistical portrait of the foreign-born population in the United States.” Pew Research Center https://www.pewresearch.org/hispanic/2019/06/03/facts-on-u-s-immigrants/ (accessed July 23, 2019).

Radin, Andrew and Clint Reach. 2017. *Russian Views of the International Order* (Santa Monica: RAND).

Rauchfleisch, Adrian and Mike S. Schafer. 2015. “Multiple public spheres of Weibo: a typology of forms and potential of online public spheres in China.” *Information, Communication and Society* 18(2) 139-155.

Reagan, Ronald. 1985. “Radio Address to the Nation on Counterintelligence Activities.” June 29 https://www.reaganlibrary.gov/research/speeches/62985a (accessed September 21, 2019).

Reshetnikov, Anatoly. 2018. “What Does Russia Mean When it Talks Greatness?” *E-International Relations*. https://www.e-ir.info/2018/05/20/what-does-russia-mean-when-it-talks-greatness/ (accessed January 19, 2020).

Richter, Felix. 2018. “Phone Ownership in the U.S.: Landline Phones Are a Dying Breed.” https://www.statista.com/chart/2072/landline-phones-in-the-united-states/ (accessed May 1, 2019).

Rid, Thomas. 2013. *Cyber War Will Not Take Place* (Oxford: Oxford University Press).

Rid, Thomas and Ben Buchanan. 2015. “Attributing Cyber Attacks.” *Journal of Strategic Studies* 38: 1-37.

Rinear, Matthew. 2015. “Armed with a Keyboard: Presidential Directive 20, Cyber-Warfare, and the International Laws of War.” *Capital University Law Review* 43: 679-720.

Ripsman, Norrin M., Jeffrey W. Taliaferro, and Steven E. Lobell. 2016. *Neoclassical Realist Theory of International Relations* (Oxford: Oxford University Press).

Risen, Tom. 2015. “Obama Signs Cybersecurity Law in Spending Package.” *U.S. News and World Report.* December 18. https://www.usnews.com/news/articles/2015-12-18/obama-signs-cybersecurity-law-in-spending-package (accessed March 3, 2020).

Roberts, Cynthia. 2010. “Russia’s BRICs Diplomacy: Rising Outsider with Dreams of an Insider.” *Polity* 42(1): 38-73.

Roberts, Kari. 2017. “Understanding Putin: The politics of identity and geopolitics in Russian foreign policy discourse.” *International Journal* 72(1): 28-55.

---. 2010. “Jets, flags, and a new Cold War? Demystifying Russia’s Arctic intentions.” *International Journal* 65(4): 957-976.

Roberts, Lawrence G. 1978. “The Evolution of Packet Switching.” *Proceedings of the IEEE* 66(11): 1307-1313.

Robinson, Michael, Kevin Jones, and Helge Janicke. 2015. “Cyber warfare: Issues and challenges.” *Computers and Security* 49: 70-94.

Rodgers, James. 2019. “Russia in 2019: Testing the Limits of Technology.” *Forbes*. December 20. https://www.forbes.com/sites/jamesrodgerseurope/2019/12/20/russia-in-2019-testing-the-limits-of-technology/#2fd8765a5b74 (accessed January 21, 2020).

Rose, Gideon. 1998. “Review: Neoclassical Realism and Theories of Foreign Policy.” Review of *The Perils of Anarchy: Contemporary Realism and International Security*, by Michael E. Brown; *Useful Adversaries: Grand Strategy, Domestic Mobilization, and Sino-American Conflict*, 1947-1958, by Thomas J. Christensen; *Deadly Imbalances: Tripolarity and Hitler’s Strategy of World Conquest*, by Randall L. Schweller; *The Elusive Balance: Power and Perceptions during the Cold War*, by William Curti Wohlforth; and *From Wealth to Power: The Unusual Origins of America’s World Role*, by Fareed Zakaria. *World Politics* 51: 144-172.

Rosenfeld, Michael J. and Reuben J. Thomas. 2012. “Searching for a Mate: The Rise of the Internet as a Social Intermediary.” *American Sociology Review* 77(4): 523-547.

Rotnem, Thomas E. 2018. “Putin’s Arctic Strategy: Collaboration or Conflict After Ukraine?” *Problems of Post-Communism* 65(1): 1-17.

RT. 2018. “Key to Russia’s greatness is strong economy & innovation – Putin.” https://www.rt.com/%20business/420783-putin-russia-economy-innovation/ (accessed January 19, 2020).

---. 2017. “’Whoever leads in AI will rule the world’: Putin to Russian children on Knowledge Day.” https://www.rt.com/news/401731-ai-rule-world-putin/ (accessed March 1, 2020).

Rudner, Martin. 2017. “’Electronic Jihad’: The Internet as Al Qaeda’s Catalyst for Global Terror.” *Studies in Conflict & Terrorism* 40 (1): 10-23.

Rumer, Eugene. 2018. “Strategic Objectives: It’s About the State.” In John R. Deni, Ed. *Current Russia Military Affairs: Assessing and Counter Russian Strategy, Operational Planning, and Modernization* (Carlisle: Strategic Studies Institute), 1-5.

Rumer, Eugene and Richard Sokolsky. 2019. “Thirty Years of U.S. Policy Toward Russia: Can the Vicious Circle Be Broken?” Carnegie Endowment for International Peace. June 20. https://carnegieendowment.org/2019/06/20/thirty-years-of-u.s.-policy-toward-russia-can-vicious-circle-be-broken-pub-79323 (accessed December 20, 2019).

Russett, Bruce. 1993. *Grasping the Democratic Peace: Principles for a Post-Cold War World* (Princeton: Princeton University Press).

Russian Cultural Centre. 2020. “About Us.” http://rccusa.org/ (accessed January 20, 2020).

Russian Federation. 2015. *Presidential Edict 683 approving appended text of “The Russian Federation’s National Security Strategy*” (Moscow: The Russian Federation).

Russian Federation. Ministry of Defence. 2019. Ministry of Defence of the Russian Federation. http://eng.mil.ru/ (accessed January 12, 2020).

---. 2018a. “Commander of Long-Range Air Force reported to Commander-in-Chief of Aerospace Forces on the implementation of Tu-160 flights in the Caribbean Sea.” https://eng.mil.ru/en/structure/forces/aerospace/news/more.htm?id=12208059@egNews (accessed January 11, 2020).

---. 2018b. “Russian drones spend about 140 thousand hours in air during operation in Syria.” http://syria.mil.ru/en/index/syria/news/more.htm?id=12184627@egNews (accessed January 20, 2020).

---. 2018c. “Turkey signs deal to procure Russian S-400.” http://eng.mil.ru/en/news_page/country/more.htm?id=12159192@egNews (accessed January 20, 2020).

---. 2015. “In the course of the last 24 hours, the Russian air group in the Syrian Arab Republic continued airstrikes against ISIS infrastructures.” http://eng.mil.ru/en/news_page/country/more.htm?id=12060572@egNews (accessed January 20, 2020).

Russian Federation. Ministry of Foreign Affairs. 2016. *The Foreign Policy Concept of the Russian Federation* (Moscow: Russian Federation). https://www.rusemb.org.uk/rp_insight/ (accessed April 2, 2020).

---. 2013. *Concept of the Foreign Policy of the Russian Federation* (Moscow: Russian Federation). https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/%20CptICkB6BZ29/content/id/122186 (accessed April 2, 2020).

Russian Orthodox Church. 2020. “Church and State.” http://www.patriarchia.ru/en/db/news/233/ (accessed January 20, 2020).

Ryabov, Andrei. 2008. “Tandemocracy in Today’s Russia.” *Russian Analytical Digest* 49(08): 2-6.

Sadri, Houman A. 2014. “Eurasian Economic Union (EEU): a good idea or a Russian takeover?” *Rivisti di Studi Politici Internationali* 81(4): 553-561.

Saivetz, Carol R. 2012. “Medvedev’s and Putin’s foreign policies. Introduction.” *Communist and Post-Communist Studies* 45: 375-377.

Sakai, Ko. 2019. “Russia is in danger of being overrun by China’s Belt and Road: A new Eurasian order is in the making, with Beijing in the driver’s seat.” *Nikkei Asian Review* August 17. https://asia.nikkei.com/Spotlight/Comment/Russia-is-in-danger-of-being-overrun-by-China-s-Belt-and-Road (accessed January 24, 2020).

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

Sanger, David E. 2018. *The Perfect Weapon: War, Sabotage, ad Fear in the Cyber Age* (New York: Crown).

Sanger, David E. and Nicole Perlroth. 2019. “U.S. Escalates Online Attacks on Russia’s Power Grid.” *The New York Times* June 15. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html (accessed March 3, 2020).

Schmitt, Eric, Ivan Nechepurenko, and CJ Chivers. 2019. “The truth about the brutal four-hour battle between Russian mercenaries and US commandos in Syria.” *Independent* 26 May https://www.independent.co.uk/news/world/battle-syria-us-russian-mercenaries-commandos-islamic-state-a8370781.html (accessed December 28, 2019).

Schmitt, Michael. 2015. “The Law of Cyber Targeting.” *Naval War College Review* 68(2): 10-29.

Schneider, William, Jr. 1987. “Nature of Soviet Global Strategy.” In Cline, Ray S., James Arnold Miller, and Roger E. Kanet, Eds. *Asia in Soviet Global Strategy* (Boulder: Westview Press), 11-16.

Schoen, Fletcher and Christopher J. Lamb. 2012. *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference* (Washington, DC: Center for Strategic Research, Institute for National Strategic Studies, National Defense University). https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf (accessed Sep 21, 2019).

Schweller, Randall. 2004. “Unanswered Threats: A Neoclassical Realist Theory of Underbalancing.” *International Security* 29(2): 159-202.

Segal, Adam. 2018. “The U.S.-China Cyber Espionage Deal One Year Later.” Council on Foreign Relations. December 06. https://www.cfr.org/report/threat-chinese-espionage (accessed May 17, 2019).

---. 2017. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: Public Affairs).

Seldin, Jeff. 2019. “Pentagon Concerned Russia Cultivating Sympathy Among US Troops.” *VOA*. December 8. https://www.voanews.com/usa/pentagon-concerned-russia-cultivating-sympathy-among-us-troops (accessed March 15, 2020).

Senate Report. 2019. *S. Prt. 115-21: Putin’s Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security* (Washington, DC: Government Printing Office).

Serle, Jack and Jessica Purkiss. 2017. “Drone Wars: The Full Data.” The Bureau of Investigative Journalism. January 1. https://www.thebureauinvestigates.com/stories/2017-01-01/drone-wars-the-full-data (accessed February 08, 2020).

Sestanovich, Stephen. 2017. "The brilliant incoherence of Trump's Foreign Policy." *The Atlantic*. May. https://www.theatlantic.com/magazine/archive/2017/05/the-brilliant-incoherence-of-trumps-foreign-policy/521430/ (accessed November 16, 2019).

Shah, Saqib. 2016. "The history of social networking." *Digital Trends.* May 14. https://www.digitaltrends.com/features/the-history-of-social-networking/ (accessed April 11, 2019).

Shanghai Cooperation Organisation (SCO). 2020. "The Shanghai Cooperation Organisation." http://eng.sectsco.org/about_sco/ (accessed January 24, 2020).

Shatalov, Sergei I. *Africa Notes: Soviet Assistance to Africa: The New Realities – May 1990* (Washington, DC: CSIS) https://www.csis.org/analysis/africa-notes-soviet-assistance-africa-new-realities-may-1990 (accessed October 05, 2019).

Shearer, Elisa. 2018. "Social media outpaces print newspapers in the U.S. as a news source." December 10 (Pew Research Center). https://www.pewresearch.org/fact-tank/2018/12/10/social-media-outpaces-print-newspapers-in-the-u-s-as-a-news-source/ (accessed May 1, 2019).

Simpson, Connor. 2013. "Head of D.C.'s Russian Cultural Center Accused of Recruiting American Spies." *The Atlantic.* https://www.theatlantic.com/national/archive/2013/10/head-dc-russian-cultural-center-accused-recruiting-spies/309616// (accessed January 20, 2020).

Singer, P.W. and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press).

Singer, P.W. and Emerson T. Brooking. 2018. *Like War: The Weaponization of Social Media*. (Boston: Houghton Mifflin Harcourt).

Singleton, Seth. 1987. "Final Report to National Council for Soviet and East European Research: The Future of Soviet Influence in Africa." 27 October. https://www.ucis.pitt.edu/nceeer/1987-628-6-Singleton.pdf (accessed October 05, 2019).

Smith, M.L.R. 2005. "Strategy in an age of 'low-intensity" warfare: why Clausewitz is still more relevant than his critics." Isabelle Duyvesteyn and Jan Angstrom, ed. *Rethinking the Nature of War: Cass Contemporary Security Studies Series* (London: Frank Cass), 28-64.

Smith, Tony. *Why Wilson Matters: The Origin of American Liberal Internationalism and Its Crisis Today* (Princeton: Princeton University Press).

Smyth, Regina and Sarah Oates. 2015. "Mind the Gap: Media Use and Mass Action in Russia." *Europe-Asia Studies* 67(2): 285-3-5.

Somerville, Heather. 2018. "Airbnb had 'substantially more' than $1 billion in quarterly revenue." *Reuters*. November 16. https://www.reuters.com/article/us-airbnb-results/airbnb-had-substantially-more-than-1-billion-in-quarterly-revenue-idUSKCN1NL270 (accessed April 29, 2019).

Souleimanov, Emil Aslan. 2019. "Russia's Policy in the Libyan Civil War: A Cautious Engagement." Middle East Policy Council. Summer. https://mepc.org/journal/russias-policy-libyan-civil-war-cautious-engagement (accessed March 7, 2020).

Southern District of New York. 2010. *United States of America v. Anna Chapman and Mikhail Semenko*, Sealed Complaint. June 25.

Spearin, Christopher. 2018. “NATO, Russia and Private Military and Security Companies.” *The RUSI Journal* 163(3): 66-72.

Statistica. 2019a. “Average annual OPEC crude oil price from 1960 to 2019 (in U.S. dollars per barrel) https://www.statista.com/statistics/262858/change-in-opec-crude-oil-prices-since-1960/ (accessed July 25, 2019).

---. 2019b. “Global digital population as of January 2019 (in millions).” https://www.statista.com/statistics/617136/digital-population-worldwide/ (accessed April 11, 2019).

---. 2019c. “Internet of Things (IoT) connected devices installed base worldwide from 2015-2025.” https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (accessed April 12, 2019).

---. 2019d. “Most popular online activities of adult internet users in the United States as of November 2017.” https://www.statista.com/statistics/183910/internet-activities-of-us-users/ (accessed April 12, 2019).

Statistica.com. 2019e. “Proposed budget of the U.S. government for cyber security in FY 2017 to 2020.” https://www.statista.com/statistics/675399/us-government-spending-cyber-security/ (accessed March 3, 2020).a

---. 2019f. “Public debt of the United States from 1990 to 2019 (in billion U.S. dollars).” https://www.statista.com/statistics/187867/public-debt-of-the-united-states-since-1990/ (accessed December 15, 2019).

---. 2019g. “Retail e-commerce sales worldwide from 2014-2021 (in billion U.S. dollars).” https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/ (accessed April 11, 2019).

---. 2019h. “Share of adults in the United States who use the internet from 2000 to 2018.” https://www.statista.com/statistics/185700/percentage-of-adult-internet-users-in-the-united-states-since-2000/ (accessed May 1, 2019).

---. 2019i. “Size of the cybersecurity market worldwide, from 2017 to 2023 (in billion U.S. dollars). https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/ (accessed May 16, 2019).

---. 2019j. “The 100 largest companies in the world by market value in 2018 (in billion U.S. dollars).” https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-value/ (accessed April 16, 2019).

---. 2019k. “Volume of data/information created worldwide from 2005 to 2025 (in zetabytes). https://www.statista.com/statistics/871513/worldwide-data-created/ (accessed April 11, 2019).

---. 2017. “Number of IoT devices in use worldwide from 2009 to 2020 (in billions units).” https://www.statista.com/statistics/764026/number-of-iot-devices-in-use-worldwide/ (accessed April 27, 2019).

Steinberg, Dmitri. 1992. “The Soviet Defence Burden: Estimating Hidden Defence Costs.” *Soviet Studies* 44(2): 237-263.

Steiner, Jutta. 2018. “What the Heck is Web 3.0 Anyway?” *Forbes* October 26. https://www.forbes.com/sites/juttasteiner/2018/10/26/what-the-heck-is-web-3-0-anyway/#2c00f6466614 (accessed April 12, 2019).

Stent, Angela. 2018. What Drives Russian Foreign Policy?” In John R. Deni, Ed. *Current Russia Military Affairs: Assessing and Counter Russian Strategy, Operational Planning, and Modernization* (Carlisle: Strategic Studies Institute), 6-9.

---. 2016. “Putin’s Power Play in Syria: How to Respond to Russia’s Intervention.” *Foreign Affairs* (January/February). https://www.foreignaffairs.com/articles/united-states/2015-12-14/putins-power-play-syria (accessed March 15, 2020).

Stockholm International Peace Research Institute (SIPRI). 2020. “Importer / Exporter TIV Tables.” http://armstrade.sipri.org/armstrade/page/values.php (accessed January 20, 2020).

---. 2019. “Importer / Exporter TIV Tables.” http://armstrade.sipri.org/armstrade/page/values.php (accessed October 04, 2019).

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

Stoner, Kathryn. 2014. “Putin’s Search for Greatness: Will Ukraine Bring Russia the Superpower Status It Seeks?” *Foreign Affairs.* March 2. https://www.foreignaffairs.com/%20articles/russia-fsu/2014-03-02/putins-search-greatness (accessed January 20, 2020).

Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn. 2015. *NIST Special Publication 800-2 (Revision 2): Guide to Industrial Control Systems (ICS) Security* (Washington, DC: Department of Commerce).

Strachan and Sibylle Scheipers, ed. 2011. *The Changing Character of War* (Oxford: Oxford University Press).

Strategic Defense Initiative: Hearings before the S. Comm. On Strategic and Theater Nuclear Forces of the Comm. on Armed Services United States Senate. 99th Cong. (1985) (statement of Dr. Fred C. Ikle, Under Secretary of Defense for Policy).

Stronski, Paul and Annie Himes. 2019. *Russia’s Game in the Balkans* (Washington, DC: Carnegie Endowment for International Peace).

Suesse, Marvin. 2001. “Breaking the Unbreakable Union: Nationalism, Disintegration and the Soviet Economic Collapse.” *The Economic Journal* 128 (November): 2933-2967.

Swain, D. Derek. 1990. “The Soviet Military Sector: How it is Defined and Measured.” In Henry S. Rowen and Charles Wolf, Jr., ed. *The Impoverished Superpower: Perestroika and the Soviet Military Burden* (San Francisco: Institute for Contemporary Studies Press), 93-109.

Symantec Corp. 2019. “Internet Security Threat Report: Executive Summary Volume 24” (February). https://docs.broadcom.com/doc/istr-24-executive-summary-en (accessed May 09, 2019).

---. 2018. “The Cyber Security Whodunnit: Challenges in Attribution of Targeted Attacks.” October 3. https://www.symantec.com/blogs/expert-perspectives/cyber-security-whodunnit-challenges-attribution-targeted-attacks (accessed May 08, 2019).

Talbott, Strobe. 2006. “Russia and the G8: Better Luck Next Year.” Brookings. June 30. https://www.brookings.edu/opinions/russia-and-the-g8-better-luck-next-year/ (accessed March 14, 2020).

Taubman, Philip. 1985. “The Shultz-Weinberger Feud.” *The New York Times Magazine*. April 14.

Tayler, Jeffrey. 2008. “The Master and Medvedev: Why Vladimir Putin’s successful effort to handpick his replacement may backfire.” *The Atlantic* 322(2). July/August. https://www.theatlantic.com/%2520magazine/archive/2008/07/the-master-and-medvedev/306840/ (accessed February 23, 2020).

Taylor, Kyle and Laura Silver. 2019. “Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally.” February 5 (Pew Research Center). https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/ (accessed May 1, 2019).

Thomas, Timothy. 2015. *Russia Military Strategy: Impacting 21st Century Reform and Geopolitics* (Ft. Leavenworth: Foreign Military Studies Office).

Thompson, Nicholas and Issie Lapowsky. 2018. “How Russian Trolls Used Meme Warfare to Divide America.” *Wired*. December 17. https://www.wired.com/story/russia-ira-propaganda-senate-report/ (accessed January 20, 2020).

Tiirmaa-Klaar. H., J. Gassen, E. Gerhards-Padilla, and P. Martini. 2013. “Botnets, Cybercrime and National Security,” 1-40. In *Botnets* (London: Springer).

Tikk, Eneken, Kadri Kaska, and Liis Vihul. 2010. *International Cyber Incidents: Legal Considerations* (Tallinn: CCDCOE).

Trachtenberg, Marc. 2018. “Assessing Soviet Economic Performance During the Cold War: A Failure of Intelligence?” *Texas National Security Review* 1(2): 76-101.

Treisman, Daniel. 2014. “Putin’s popularity since 2010: why did support for the Kremlin plunge, then stabilize?” *Post-Soviet Affairs* 30(5): 370-388.

Trenin, Dmitri. 2016. “The Revival of the Russian Military: How Moscow Reloaded.” *Foreign Affairs* 95(3): 23-29.

Tsygankov, Andrei P. 2011. “Preserving Influence in a Changing World: Russia’s Grand Strategy.” *Problems of Post-Communism* 58(2): 28-44.

Union of Soviet Socialist Republics (USSR). 1977. *USSR Constitution*. October 7. http://www.departments.bucknell.edu/russian/const/77cons01.html#I (accessed August 30, 2019).

United Kingdom. 2018. Foreign and Commonwealth Office. *UK and allies reveal global scale of global Chinese cyber campaign.* December 20. https://www.gov.uk/government/news/%20uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign (accessed May 3, 2019).

United Nations (UN). 2019a. "Country Data." https://data.un.org/ (accessed May 2, 2019).

---. 2018. "E-Government Development Index (EGDI). https://www.un.org/development/desa/publications/2018-un-e-government-survey.html (accessed May 2, 2019).

---. Department of Economic and Social Affairs. 2017. *E-Government for Sustainable Development: Report of the Expert Group Meeting* (New York: United Nations). http://workspace.unpan.org/sites/internet/Documents/UNPAN97610.pdf (accessed May 2, 2019).

---. Group of Governmental Experts (UN GGE). 2013. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98*, 24 June 2013. https://www.un.org/en/ga/search/view_doc.asp?symbol=A/68/98 (accessed May 1, 2019).

United States Agency for International Development (USAID). 2020a. "Democracy, Human Rights and Governance." https://www.usaid.gov/democracy (accessed March 31, 2020).

---. 2020b. "Foreign Aid Explorer." https://explorer.usaid.gov/ (accessed February 22, 2020).

---. 2017. *U.S. Overseas Loans and Grants: Obligations and Loan Authorizations, July 1, 1945–September 30, 2017* (Washington, DC: USAID). https://explorer.usaid.gov/reports (accessed August 28, 2019).

United States Bureau of Labor Statistics. 2019. "Databases, Tables & Calculators by Subject." https://www.bls.gov/data/ (accessed June 2, 2019).

United States Census Bureau. 2018. *National Population Totals and Components of Change: 2010-2018* (Washington, DC: US Census Bureau). https://www.census.gov/data/tables/%20time-series/%20demo/popest/2010s-national-total.html (accessed May 1, 2019).

---. 1980. *Decennial Census of Population and Housing* (Washington, DC: US Census Bureau). https://www.census.gov/programs-surveys/decennial-census/decade.1980.html (accessed May 1, 2019).

United States Congress. 2018. House of Representatives, Permanent Select Committee on Intelligence. 2018. *Report on Russian Active Measures*. March 22.

---. 2016. *Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden*.

United States Cyber Command. 2020. “U.S. Cyber Command: History.” https://www.cybercom.mil/About/History/ (accessed March 3, 2020).

United States Defense Intelligence Agency (DIA). 2019. *Challenges to Security in Space* (Washington, DC: DIA).

---. 2017. *Russia Military Power: Building A Military to Support Great Power Aspirations* (Washington, DC: DIA).

United States Department of Defense (DOD). 2018a. *Nuclear Posture Review* (Washington, DC: Department of Defense).

---. 2018b. *Summary of the National Defense Strategy of the United States of America* (Washington, DC: Department of Defense).

---. 2017. “Department of Defense Press Briefing by Colonel Dillon via teleconference from Baghdad, Iraq.” https://www.defense.gov/Newsroom/%20Transcripts/Transcript/Article/1345953/ %20department-of-defense-press-briefing-by-colonel-dillon-via-teleconference-from/ (accessed December 15, 2019).

---. 2016. “3rd Offset Strategy 101: What it is, What the Tech Focuses Are.” https://www.dodlive.mil/2016/03/30/3rd-offset-strategy-101-what-it-is-what-the-tech-focuses-are/ (accessed March 1, 2020).

---. 2010. *Nuclear Posture Review* (Washington, DC: Department of Defense).

---. 2008. “Defense Casualty Analysis System: DCAS Vietnam Conflict Extract File record counts by INCIDENT OR DEATH DATE (Year) (as of April 29, 2008) https://www.archives.gov/research/military/vietnam-war/casualty-statistics (accessed June 2, 2019).

---. 1990. *Soviet Military Power 1990* (Washington, DC: Department of Defense).

---. 1989. *Soviet Military Power: Prospects for Change 1989* (Washington, DC: DOD).

United States Department of Defense, Defense Manpower Data Center (DMDC). 2018. Defense Manpower Data Center. *Counts of Active Duty and Reserve Service Members and APF Civilians* (Washington, DC: Department of Defense).

---. 2016. *Counts of Active Duty and Reserve Service Members and APF Civilians* (Washington, DC: Department of Defense).

---. 2012. *Counts of Active Duty and Reserve Service Members and APF Civilians* (Washington, DC: Department of Defense).

---. 2010. *Counts of Active Duty and Reserve Service Members and APF Civilians* (Washington, DC: Department of Defense).

---. 2008. *Counts of Active Duty and Reserve Service Members and APF Civilians* (Washington, DC: Department of Defense).

---. 2000. *Worldwide Manpower Distribution by Geographical Area* (Washington, DC: Department of Defense).

---. 2005. *Worldwide Manpower Distribution by Geographical Area* (Washington, DC: Department of Defense).

---. 1998. *Active Duty Military Personnel Strengths by Regional Area and by Country* (Washington, DC: Department of Defense).

---. 1992. *Active Duty Military Personnel Strengths by Regional Area and by Country* (Washington, DC: Department of Defense).

---. 1988. *Department of Defense Military Personnel on Active Duty by Grade in Which Serving. September 30* (Washington, DC: DMDC). https://www.dmdc.osd.mil/appj/dwp/dwp_reports.jsp (accessed July 6, 2019).

---. 1985. *Soviet Military Power 1985* (Washington, DC: Department of Defense).

---. 1980. *Department of Defense Military Personnel on Active Duty by Grade in Which Serving. September 30* (Washington, DC: DMDC).

---. 1979. *Department of Defense Military Personnel on Active Duty By Grade in Which Serving* (Washington, DC: DMDC).

---. 1970. *Department of Defense Deployment of Military Personnel by Country* (Washington, DC: DMDC).

---. 1968. *Department of Defense Military Personnel on Active Duty By Grade in Which Serving* (Washington, DC: DMDC).

---. 1950. *Department of Defense Deployment of Military Personnel by Country. As of 30 June* (Washington, DC: DMDC).

United States Department of Defense (DOD). Defense Security Cooperation Agency. 2020. "Defense Institution of International Legal Studies." https://www.dsca.mil/programs/defense-institute-international-legal-studies-diils (accessed March 31, 2020).

United States Department of Homeland Security. 2016. *Strategic Principles for Securing the Internet of Things* (Washington, DC: Department of Homeland Security).

United States Department of Homeland Security. CISA. 2018. "Alert (TA18-106A): Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices." April 16. https://www.us-cert.gov/ncas/alerts/TA18-106A (accessed January 22, 2020).

United States Department of Justice. 2020. "International Criminal Investigative Training Assistance Program (ICITAP)." https://www.justice.gov/criminal-icitap (accessed March 31, 2020).

United States Department of State. 2020a. “Global Engagement Center.” https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/ (accessed February 29, 2020).

---. 2020b. “Crimea is Ukraine.” https://www.state.gov/crimea-is-ukraine-3/ (accessed February 29, 2020).

---. 2019a. “The Global Coalition To Defeat ISIS.” https://www.state.gov/bureaus-offices/bureaus-and-offices-reporting-directly-to-the-secretary/the-global-coalition-to-defeat-isis/ (accessed December 15, 2019).

---. 2019b. “U.S. Relations With Russia.” June 25. https://www.state.gov/u-s-relations-with-russia/ (accessed March 15, 2020).

---. 2018. “Russia 2018 Human Rights Report.” https://www.state.gov/wp-content/uploads/2019/03/RUSSIA-2018-HUMAN-RIGHTS-REPORT.pdf (accessed March 31, 2020).

---. 2017. “Ukraine and Russia Sanctions.” https://www.state.gov/ukraine-and-russia-sanctions/ (accessed February 22, 2020).

---. 2013. “Russia 2012 Human Rights Report.” https://2009-2017.state.gov/documents/%20organization/204543.pdf (accessed March 31, 2020).

---. 2010. “List of Umbrella Science and Technology Agreements.” https://2009-2017.state.gov/e/oes/rls/fs/2009/140665.htm (accessed April 1, 2020).

---. 2008. “2007 Country Reports on Human Rights Practices: Russia.” https://2009-2017.state.gov/j/drl/rls/hrrpt/2007/100581.htm (accessed March 31, 2020).

---. 1987. *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986-1987* (Washington, DC: Department of State).

---. 1981. Press Conference by The Honorable Alexander M. Haig, Jr. No. 25. January 28. https://www.reaganlibrary.gov/sites/default/files/digitallibrary%20/smof/cos/bakerjames/box-002/40-028-6914302-002-011-2016.pdf (accessed August 14, 2019).

United States District Court Southern District of New York (SDNY). 2016. “United States of America v. Ahmad Fathi, Hamid Firoozi, Amin Shokohi, Sadegh Ahmadzadegan, a/k/a “Nitr0jen26,” Omid Ghaffarinia, a/k/a “PLuS,” Sina Keissar, and Nder Saedi, a/ka “Turk Server.” Indictment. 16 Cr. 48 (S.D.N.Y. Jan. 21, 2016).

United States National Institute of Standards and Technology (NIST). 2018. *Cybersecurity Framework: History and Creation of the Framework*. https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework (accessed March 15, 2019).

United States Office of the Director of National Intelligence (DNI). 2019. *Worldwide Threat Assessment of the US Intelligence Community* (Washington, DC: Director of National Intelligence).

---. 2018. *Foreign Economic Espionage in Cyberspace* (Washington, DC: Director of National Intelligence).

---. 2017a. "Background to 'Assessing Russian Activities and Intentions in Recent US Elections:' The Analytic Process and Cyber Incident Attribution" (Washington, DC: Director of National Intelligence). https://www.dni.gov/files/documents/ICA_2017_01.pdf (accessed March 1, 2019).

---. 2017b. *Software Supply Chain Attacks* (Washington, DC: ODNI). https://www.dni.gov/files/NCSC/documents/%20supplychain/20190327-Software-Supply-Chain-Attacks02.pdf (accessed May 9, 2019).

---. 2014. "Fact Sheet: President Putin's Fiction: 10 False Claims About Ukraine." https://2009-2017.state.gov/r/pa/prs/ps/2014/03/222988.htm (accessed March 15, 2020).

---. 2012. "U.S. Russia Economic Cooperation." https://2009-2017.state.gov/p/eur/rls/fs/193103.htm (accessed March 15, 2020).

---. 2008. "Secretary Rice Addresses U.S.-Russia Relations At the German Marshall Fund." https://2001-2009.state.gov/secretary/rm/2008/09/109954.htm (accessed March 15, 2020).

United States Postal Service (USPS). 2019. "2019 Postal Facts Companion." https://facts.usps.com/wp-content/uploads/2019_POSTAL_FACTS_WEB_COMPANION.pdf (accessed May 1, 2019).

United States Senate. 2016. *Testimony Before the Senate Appropriations Subcommittee on Defense*.

Varghese, Robin. 2018. "Marxist World: What Did You Expect From Capitalism?" *Foreign Affairs* 97(4): 34-42.

Veebel, Viljar and Illimar Ploom. 2016. "Estonian Perceptions of Security: Not only About Russia and the Refugees." *Journal of Baltic Security* 2(2): 35-70.

Venables, Adrian, Siraj Ahmed Shaikh, and James Shuttleworth. 2017. "The Projection and Measurement of Cyberpower." *Security Journal* 30(3): 1000-1011.

Verick, Sher and Iyanatul Islam. 2010. *Discussion Paper No 4934. The Great Recession of 2008-2009: Causes, Consequences and Policy Responses* (Bonn: Institute for the Study of Labor) http://ftp.iza.org/dp4934.pdf (accessed December 14, 2019).

Walker, Scott. 2018. *The Long Hangover: Putin's New Russia and the Ghosts of the Past* (New York: Oxford University Press).

Walt, Steven M. 1987. *The Origins of Alliances* (Ithaca: Cornell University Press).

Waltz, Kenneth N. 1979. *Theory of International Politics* (London: McGraw Hill).

---. 1954. *Man, the State, and War: a theoretical analysis* (New York: Columbia University Press).

Webb, Greg. 2019. "Russian Weapons Accident Raises Nuclear Concerns." *Arms Control Today* 49(7): 29-30.

Weir, Fred. 2011. "Could Putin and Medvedev face off in an open Russian election?" *The Christian Science Monitor*. https://www.csmonitor.com/World/Europe/2011/0420/Could-Putin-and-Medvedev-face-off-in-an-open-Russian-election (accessed December 14, 2019).

Werner, Ben. "Navy, Marines Tell Congress Emphasis on Arctic is Growing." *U.S. Naval Institute Press*. March 5.

The White House. 2018a. "Cybersecurity Funding." https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf (accessed May 15, 2019).

---. 2018b. *Fact Sheets: Artificial Intelligence for the American People.* (Washington, DC: White House).

---. 2017. *National Security Strategy of the United States of America* (Washington, DC: White House).

---. 2016. *Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment* (Washington, DC: White House). https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity (accessed March 15, 2020).

---. 2015. *National Security Strategy of the United States of America* (Washington, DC: White House).

---. 2014a. *FACT SHEET: U.S. Support and Reassurance Initiatives for the Baltics and Central Europe* (Washington, DC: White House).

---. 2014b. *Readout of President Obama's Call with President Putin* (Washington, DC: White House).

---. 2010. *National Security Strategy of the United States of America* (Washington, DC: White House).

---. 2006. *National Security Strategy of the United States of America* (Washington, DC: White House).

---. 2002. *National Security Presidential Directive/NSPD-23: National Policy on Ballistic Missile Defense* (Washington, DC: White House). https://www.georgewbushlibrary.smu.edu/ (accessed February 22, 2020).

---. 2013. "Presidential Policy Directive – Critical Infrastructure Security and Resilience (PPD-21)." https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed May 15, 2019).

---. 1994. *Presidential Decision Directive / NSC-25: U.S. Policy on Reforming Multilateral Peace Operations* (Washington, DC: White House). https://clinton.presidentiallibraries.us/items/%20show/%2012749 (accessed November 30, 2019).

---. 1988a. *National Security Decision Directive Number 320: National Policy on Strategic Trade Controls.* November 20. https://www.reaganlibrary.gov/sites/default/files/%20archives/reference/scanned-nsdds/nsdd320.pdf (accessed October 26, 2019).

---. 1988b. *National Security Decision Directive Number 311: US-Soviet Defense and Military Relations*. July 29. https://www.reaganlibrary.gov/sites/default/files/archives/reference%20/scanned-nsdds/nsdd311.pdf (accessed October 26, 2019).

---. 1988c. *National Security Decision Directive Number 305: Objectives at the Moscow Summit*. April 26. https://www.reaganlibrary.gov/sites/default/files/archives/reference/scanned-nsdds/nsdd305.pdf (accessed October 26, 2019).

---. 1987a. *National Security Decision Directive Number 270: Afghanistan.* May 1. https://www.reaganlibrary.gov/sites/default/files/archives/reference/scanned-nsdds/nsdd270.pdf (accessed October 26, 2019).

---. 1987b. *National Security Decision Directive Number 260: Soviet Noncompliance with Arms Control Agreements*. February 17. https://www.reaganlibrary.gov/sites/default/files/archives/%20reference/scanned-nsdds/nsdd260.pdf (accessed October 26, 2019).

---. 1986a. *National Security Decision Directive Number 252: ICBM Modernization.* December 24. https://www.reaganlibrary.gov/sites/default/files/archives/reference/scanned-nsdds/nsdd252.pdf (accessed October 26, 2019).

---. 1986b. *National Security Decision Directive Number 245: Reagan-Gorbachev Preparatory Meeting.* October 7. https://www.reaganlibrary.gov/sites/default/files/archives/reference/%20scanned-nsdds/nsdd245.pdf (accessed October 26, 2019).

---. 1986c. *National Security Decision Directive Number d: Basic National Security Strategy*. September 2. https://www.reaganlibrary.gov/sites/default/files/archives/reference/scanned-nsdds/nsdd238.pdf (accessed August 14, 2019).

---. 1986d. *National Security Decision Directive Number 223: Implementing the Geneva Exchanges Initiative*. April 22. https://www.reaganlibrary.gov/sites/default/files%20/archives/reference/scanned-nsdds/nsdd223.pdf (accessed August 14, 2019).

---. 1986e. *National Security Decision Directive Number 222: Consultations on U.S. Interim Restraint Policy.* April 21. https://www.reaganlibrary.gov/sites/default/files/archives/reference/%20scanned-nsdds/nsdd222.pdf (accessed October 26, 2019).

---. 1985a. *National Security Decision Directive Number 194: Meeting with Soviet Leader in Geneva: Themes and Perceptions*. October 25. https://www.reaganlibrary.gov/sites/default/files/%20archives/reference/scanned-nsdds/nsdd194.pdf (accessed July 23, 2019).

---. 1985b. *National Security Decision Directive Number 189: National Policy on the Transfer of Scientific, Technical and Engineering Information.* September 21. https://www.reaganlibrary.gov/sites/default/files/archives/reference/scanned-nsdds/nsdd189.pdf (accessed October 26, 2019).

---. 1985c. *National Security Decision Directive Number 161: Soviet Noncompliance with Arms Control Agreements.* February 6. https://www.reaganlibrary.gov/sites/default/files/archives/%20reference/%20scanned-nsdds/nsdd161.pdf (accessed October 26, 2019).

---. 1985d. *National Security Decision Directive Number 153: Instructions for the Shultz-Gromyko Meeting in Geneva.* January 1. https://www.reaganlibrary.gov/sites/default/files/%20archives/reference/scanned-nsdds/nsdd153.pdf (accessed October 26, 2019).

---. 1984a. *National Security Decision Directive Number 137: US Nuclear Arms Control Strategy for 1984* March 31. https://www.reaganlibrary.gov/sites/default/files/archives/reference/scanned-nsdds/nsdd137.pdf (accessed July 18, 2019).

---. 1984b. *National Security Decision Directive Number 130: US International Information Policy*. https://www.reaganlibrary.gov/sites/default/files/archives/reference/scanned-nsdds/nsdd130.pdf (accessed October 26, 2019).

---. 1984c. *National Security Decision Directive Number 124: Central America: Promoting Democracy, Economic Improvement, and Peace.* February 7. https://www.reaganlibrary.gov/sites/default/files/archives/reference/scanned-nsdds/nsdd130.pdf (accessed October 26, 2019).

---. 1983a. *National Security Decision Directive Number 165: Instructions for the First Round of US/Soviet Negotiations in Geneva.* Undated. https://www.reaganlibrary.gov/sites/default/files/%20archives/reference/scanned-nsdds/nsdd165.pdf (accessed October 26, 2019).

---. 1983b. *National Security Decision Directive Number 105: Eastern Caribbean Regional Security Policy*. October 4. https://www.reaganlibrary.gov/sites/default/files/archives/reference/%20scanned-nsdds/nsdd105.pdf (accessed October 26, 2019).

---. 1983c. *National Security Decision Directive Number 102: U.S. Response to Soviet Destruction of KAL Airliner.* https://www.reaganlibrary.gov/sites/default/files/archives/%20reference/scanned-nsdds/nsdd102.pdf *(accessed October 26, 2019).*

---. 1983d. *National Security Decision Directive Number 100: Enhanced U.S. Military Activity and Assistance for the Central American Region.* July 28. https://www.reaganlibrary.gov/sites%20/default%20/%20files/%20%20archives%20/%20reference/scanned-nsdds/nsdd100.pdf (accessed October 26, 2019).

---. 1983e. *National Security Decision Directive Number 99: United States Security Strategy for the Near East and South Asia.* July 12. https://www.reaganlibrary.gov/sites/default/files/archives/%20reference/scanned-nsdds/nsdd99.pdf (accessed October 26, 2019).

---. 1983f. *National Security Decision Directive Number 86: U.S. Approach to INF Negotiations*. March 28. https://www.reaganlibrary.gov/sites/default/files/archives/reference/scanned-nsdds/nsdd86.pdf (accessed October 26, 2019).

---. 1983g. *National Security Decision Directive Number 82: U.S. Policy Initiatives to Improve Prospects for Victory in El Salvador.* February 24. https://www.reaganlibrary.gov/sites/default/%20files/archives/reference/scanned-nsdds/nsdd82.pdf (accessed October 26, 2019).

---. 1983h. *National Security Decision Directive Number 75: US Relations with the USSR*. January 17. https://www.reaganlibrary.gov/sites/default/files/archives/reference/scanned-nsdds/nsdd75.pdf (accessed August 14, 2019).

---. 1982a. *National Security Decision Directive Number 71: U.S. Policy Toward Latin Americ In the Wake of the Falklands Crisis.* November 30. https://www.reaganlibrary.gov/sites/default/%20files/archives/reference/scanned-nsdds/nsdd71.pdf (accessed October 26, 2019).

---. 1982b. *National Security Decision Directive Number 70: Nuclear Capable Missile Technology Transfer Policy*. November 10. https://www.reaganlibrary.gov/sites/default/files/%20archives/reference/scanned-nsdds/nsdd70.pdf (accessed October 26, 2019).

---. 1982c. *National Security Decision Directive Number 69: The M-X Program.* November 22. https://www.reaganlibrary.gov/sites/default/files/%20archives/reference/scanned-nsdds/nsdd70.pdf (accessed October 26, 2019).

---. 1982d. *National Security Decision Directive Number 59: Cuba and Central America.* October 5. https://www.reaganlibrary.gov/sites/default/files/archives/reference/scanned-nsdds/nsdd59.pdf (accessed October 26, 2019).

---. 1982e. *National Security Decision Directive Number 57: United States Policy Towards the Horn of Africa.* September 17. https://www.reaganlibrary.gov/sites/default/files/archives/%20reference/scanned-nsdds/nsdd57.pdf (accessed October 26, 2019).

---. 1982f. *National Security Decision Directive Number 54: United States Policy Toward Eastern Europe.* September 2. https://www.reaganlibrary.gov/sites/default/files/archives/reference/scanned-nsdds/nsdd130.pdf%20scanned-nsdds/nsdd54.pdf (accessed October 26, 2019).

---. 1982g. *National Security Decision Directive Number 45: United States International Broadcasting*. July 15. https://www.reaganlibrary.gov/sites/default/files/archives/reference/%20scanned-nsdds/nsdd45.pdf (accessed October 26, 2019).

---. 1982h. *National Security Decision Directive Number 41: December 30, 1981 Sanctions on Oil and Gas Equipment Exports to the Soviet Union.* June 22. https://www.reaganlibrary.gov/sites/%20default/files/archives/reference/scanned-nsdds/nsdd41.pdf (accessed October 26, 2019).

---. 1982i. *National Security Decision Directive Number 32: U.S. National Security Strategy*. May 20. https://www.reaganlibrary.gov/sites/default/files/archives/reference/scanned-nsdds/nsdd32.pdf (accessed October 26, 2019).

Wike, Richard. 2011. "Changing Global Perceptions of the U.S. in the Post-Sept. 11 Era: From Hyperpower to Declining Power." https://www.pewresearch.org/global/2011/09/07/from-hyperpower-to-declining-power/ (accessed December 07, 2019).

Wilson, James Graham. 2007. "How Grand Was Reagan's Grand Strategy, 1976-1984?" *Diplomacy and Statecraft* 18: 773-803.

World Bank. 2019a. "China – GDP (Current US$)." https://data.worldbank.org/country/china (accessed December 01, 2019).

---. 2019b. “GDP growth (annual %) – Russian Federation.” https://data.worldbank.org/indicator/%20NY.GDP.MKTP.KD.ZG?locations=RU (accessed December 14, 2019).

---. 2019c. “GDP growth (annual %) – United States.” https://data.worldbank.org/indicator/%20NY.GDP.MKTP.KD.ZG?locations=US (accessed November 30, 2019).

---. 2019d. “Individuals using the Internet (% of population).” https://data.worldbank.org/indicator/IT.NET.USER.ZS (accessed April 30, 2019).

---. 2019e. “Inflation, GDP deflator” (annual %). https://data.worldbank.org/indicator/%20NY.GDP.DEFL.KD.ZG?locations=US (accessed July 6, 2019).

---. 2019f. “Japan – GDP (Current US$). https://data.worldbank.org/country/japan (accessed December 01, 2019).

---. 2019g. “Military Expenditure (Current US$). https://data.worldbank.org/indicator/ms.mil.xpnd.gd.zs (accessed February 22, 2020)

---. 2019h. “Military expenditure (Current USD) – Russian Federation.” https://data.worldbank.org/indicator/MS.MIL.XPND.CD?locations=RU (accessed December 01, 2019).

---. 2019i. “Military expenditure (Current USD) – United States.” https://data.worldbank.org/indicator/MS.MIL.XPND.CD?locations=US (accessed November 24, 2019).

---. 2019j. “Russian Federation – GDP (Current US$). https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=RU (accessed December 01, 2019).

---. 2019k. “Russia Trade.” https://wits.worldbank.org/countrysnapshot/en/RUSSIA (accessed January 18, 2020).

---. 2019l. “United States – GDP (Current US$).” https://data.worldbank.org/country/united-states (accessed November 30, 2019).

World Economic Forum. 2018. “The Global Competitiveness Report.” https://reports.weforum.org/global-competitiveness-report-2018/country-economy-profiles/?doing_wp_cron=1587741633.1547338962554931640625 (accessed March 21, 2020).

---. 2013. *The Global Competitiveness Report* (Geneva: World Economic Forum). http://www3.weforum.org/docs/WEF_GlobalCompetitivenessReport_2013-14.pdf (accessed March 21, 2020).

---. 2008. *The Global Competitiveness Report* (Geneva: World Economic Forum). http://www3.weforum.org/docs/WEF_GlobalCompetitivenessReport_2008-09.pdf (accessed March 21, 2020).

Worldwide Web Consortium (W3C). 2017. *W3C Mission*. https://www.w3.org/Consortium/ (accessed April 1, 2019).

Yakovlev, Alexander N. 1985. “Тезисы к выступлению А.Н. Яковлева на совещании в ЦК КПСС руководителей средств массовой информации” (“Speech at a meeting of media executives at the Central Committee of the CPSU”) Trans. DeepL.com.. https://www.alexanderyakovlev.org/fond/issues-doc/1023327 (accessed June 12, 2019).

Yaraghi, Niam and Shamika Ravi. 2017. *The Current and Future State of the Sharing Economy* (New Delhi: Brookings).

Yegin, Mehmet. 2019. “Turkey between NATO and Russia: The Failed Balance.” *SWP Comment* June: 1-4. https://www.swp-berlin.org/10.18449/2019C30/ (accessed January 24, 2020).

York, Dan. 2019. “Celebrating 50 Years of the RFCs That Define How the Internet Works.” https://www.internetsociety.org/blog/2019/04/celebrating-50-years-of-the-rfcs-that-define-how-the-internet-works/ (accessed April 11, 2019).

Zakaria, Fareed. 1998. *From Wealth to Power: The Unusual Origins of America’s World Role* (Princeton: Princeton University Press).

Zubok, Vladislav M. “Soviet foreign policy from détente to Gorbachev, 1975-1985.” In Leffler, Melvyn P. and Odd Arne Westad, Ed. 2010. *The Cambridge History of the Cold War, Vol III*. Cambridge: Cambridge University Press, 89-111.

---. 2009. *A Failed Empire: The Soviet Union in the Cold War from Stalin to Gorbachev* (Chapel Hill: The University of North Carolina Press).

Zygar, Mikhail. 2016. *All the Kremlin’s Men: Inside the Court of Vladimir Putin* (New York: Public Affairs).