# Cyber Operations and Its Impact on State Sovereignty: A Comparative Analysis of Electoral Interference

Stolwijk, Arnold


Universiteit Leiden
The Netherlands

# Cyber Operations and Its Impact on State Sovereignty:

## A Comparative Analysis of Electoral Interference

Arnold Stolwijk
Student Number: s2649608
Email: a.a.stolwijk@umail.leidenuniv.nl
Faculty of Humanities, Leiden University

MA Thesis International Relations: Global Conflict in the Modern Era
Supervisor: Dr. Lukas Milevski
Second Reader: Dr. Chiara Libiseller
January 31, 2025

Word Count: 13.246

## Abstract

This thesis investigates the impact of cyber operations on state sovereignty through a comparative analysis of CIA electoral interference in Chile and Russian interference in the 2016 US elections. It examines whether cyber operations represent a novel challenge to sovereignty or a continuation of longstanding state practices. Employing a realist framework, the research argues that while technological advancements have transformed the tools of covert interference, the underlying objectives and strategies remain consistent. The findings reveal a continuity in state behavior, where cyber operations serve as modern extensions of traditional methods of political manipulation. This study highlights the adaptability of sovereignty in response to emerging challenges, asserting that its fundamental principles endure despite shifts in the technological landscape. The research contributes to the discourse on cyber operations, demonstrating their role as an evolution rather than a disruption in the practice of statecraft.

# Table of Contents

# 1. Introduction

State sovereignty has been foundational to International Relations (IR) for centuries, defining how states interact with each other and shaping the international system itself. The concept of sovereignty was strongly influenced by key thinkers such as Jean Bodin and Thomas Hobbes. Bodin, in his work *Six Books of the Commonwealth* (1576), emphasized the indivisibility and absoluteness of sovereignty, arguing that it should reside with a single, supreme authority (Bodin 1955, 25). Hobbes shared a similar concept of sovereignty in his book *Leviathan* (1651), in which he viewed sovereign power as essential for maintaining peace and security, a necessary force to escape the chaos of the state of nature (Hobbes 1651, 103-104). Together, their ideas solidified sovereignty as a pillar of stability and order in IR. Over time, the concept of sovereignty has evolved, adapting to changes in the international environment. One significant historical moment frequently referred to when discussing the origins of sovereignty is the Peace of Westphalia in 1648. In IR, this treaty, which ended the Thirty Years' War, has often been considered foundational for the modern concept of sovereignty (Krasner 1995, 115). This notion can mostly be attributed to an influential article published by Leo Gross in 1948, in which he claims: "The Peace of Westphalia, for better or worse, marks the end of an epoch and the opening of another […] In the political field it marked man's abandonment of the idea of a hierarchical structure of society and his option for a new system characterized by a multitude of states, each sovereign within its territory, equal to one another, and free from any external sovereignty" (Gross 1948, 28-29). However, the "Westphalian model" has become a debated topic in recent decades, with several scholars dismissing it as a myth (Krasner 1995; Osiander 2001; Beaulac 2020). Despite the debate, the Peace of Westphalia is perhaps still a pivotal moment in the history of sovereignty, as it could be seen as the consolidation of fragmented elements of sovereignty that had been around for centuries (Philpott 2010, 77). It is for this reason that this thesis will refer to the Westphalian model, as it is described by Gross, when discussing this traditional concept of sovereignty. Nowadays, sovereignty is often defined as the absolute authority of a state over its territory and internal affairs, free from external interference (Afyare 2024, 1658).

Challenges such as globalization and rapid technological advancements have complicated the exercise of state sovereignty (Sassen 1996, xxi-xxii). Among these challenges, cyber operations have emerged as a significant test to the traditional understanding of sovereignty. The interconnected and borderless nature of cyberspace, in this thesis referring to

“the virtual computer world, specifically an electronic medium used to facilitate interactions and communication across a global network of interconnected systems” (Beal 2024), allows both state and non-state actors to interfere in the domestic affairs of others without physically crossing borders (Chatinakrob 2024, 27). This raises an important question: do cyber operations represent a fundamental shift in the concept of sovereignty, or are they simply a new manifestation of long-standing state behavior?

This thesis addresses the research problem of whether cyber operations fundamentally alter state sovereignty or are better understood as a continuation of traditional interstate actions. Much of the current literature frames cyber operations as an unprecedented challenge to sovereignty, emphasizing the difficulties of attribution, enforcement, and jurisdiction in the digital realm. Cyberspace's cross-border nature is said to challenge the territoriality and exclusivity central to the concept of sovereignty, as cyber activities often occur across multiple borders or in international spaces, conducted by individuals or entities subject to various jurisdictions (Mueller 2020, 780). However, this perspective may overlook crucial historical continuities in how states interact and undermine each other's sovereignty. Throughout history, states have used covert actions and sabotage to achieve strategic objectives, which suggests that cyber operations may not be a fundamentally new threat but rather an evolution of established state practices. Covert actions in this thesis is defined as “a spectrum of coordinated coercive measures, short of direct military assault, secretly exercised by one state in order to influence the sovereign affairs of another” (Berkeley La Raza Law Journal 1984, 139).

The central research question guiding this thesis is: "To what extent has state sovereignty evolved in the context of interstate cyber operations in peacetime, and how does it compare with interstate actions prior to the cyber era?" By addressing this question, the thesis aims to determine whether cyber operations, as exemplified by the Russian meddling in the 2016 United States (US) elections, represent a new type of challenge to sovereignty or if they should be seen as part of a historical continuum, akin to the Central Intelligence Agency’s (CIA) interference in Chile during the Cold War. This comparative approach will help clarify whether the principles of state sovereignty are facing a fundamentally new challenge or merely adapting to new technological realities.

It will be argued that cyber operations do not represent a novel challenge to sovereignty but rather continue the historical pattern of interstate sabotage. By comparing two cases of interstate sabotage operations during peacetime, this research argues that states have consistently used covert means to achieve strategic goals, regardless of the available

technologies. The continuity of these practices demonstrates that while tools and methods evolve, the underlying principles of sovereignty and state behavior remain largely unchanged.

The focus of the thesis is on interstate cyber operations during peacetime, specifically how these operations compare with historical forms of sabotage. By narrowing the scope to peacetime activities, the research highlights the subtleties of sovereignty challenges that do not involve open warfare but still significantly impact state control and autonomy. The comparative analysis is grounded in the theoretical perspective of realism, which emphasizes the inherent competition among states and their pursuit of power and security (Korab-Karpowicz 2010, 1). Realism provides a suitable framework for understanding both historical and modern cases as expressions of state behavior aimed at maximizing strategic advantage.

An outline of the thesis structure is as follows: Chapter 2 presents a comprehensive literature review, examining the challenges posed by globalization and cyber operations, and the current scholarly debate on the erosion or continuity of sovereignty. Chapter 3 outlines the methodology, explaining the comparative case study approach and justifying the selection of the two cases of election interference as case studies. Chapters 4 provides a detailed analysis of these two cases, drawing comparisons to highlight the continuity of state actions. Chapter 5 discusses the broader implications of the findings for the concept of sovereignty in the modern era, while Chapter 6 concludes the thesis.

By comparing historical and modern forms of election interference, this thesis challenges the view that cyber operations represent a novel threat to sovereignty. Instead, it argues for a perspective that emphasizes continuity and adaptation. This approach not only provides a deeper understanding of sovereignty in the digital age but also highlights the enduring nature of state strategies in maintaining power and control.

## 2. Literature Review

In examining the existing literature on cyber operations and sovereignty, a division becomes visible among scholars. On one hand, some argue that cyber operations represent a fundamentally novel challenge that cannot be adequately addressed within traditional frameworks, thereby posing a significant threat to state sovereignty. On the other hand, others contend that cyber operations are compatible with existing legal and theoretical frameworks, suggesting that they do not constitute a new threat to sovereignty. This literature review aims to explore both perspectives on cyber operations and sovereignty to provide the necessary

context to justify the focus of this research, which seeks to determine whether cyber operations genuinely represent a novel challenge to sovereignty or align with traditional forms of state behavior.

### 2.1 Challenges to Sovereignty: Globalization and Cyber Operations

As discussed in the introduction chapter of this thesis, the traditional concept of sovereignty, being the absolute authority of a state over its territory and internal affairs, free from external interference, has faced numerous challenges over the centuries, particularly with the advent of globalization and technological advancements. Sassen (1996) states that globalization has led to the partial denationalization of national territory, making it increasingly difficult for states to maintain control over transborder flows of goods, people, and information. She argues that globalization has eroded the ability of states to exercise control over their territories, as economic and social processes increasingly operate beyond the reach of national governments (xxii). This has led to a reconfiguration of state sovereignty, where the authority of the state is no longer absolute but is shared with transnational actors and institutions. In recent years, cyber operations have emerged as a significant challenge to the traditional notion of sovereignty. The rise of cyberspace as a new domain of interaction has enabled both state and non-state actors to interfere in the internal affairs of other states without physically crossing borders.

Margulies (2013) discusses how cyber operations challenge the law of state responsibility, particularly because private actors being involved, and that adaptations should be made (496). He argues that traditional legal frameworks, such as the “effective control” test used to establish state responsibility for kinetic attacks, are inadequate for addressing cyber operations due to the complexities of attribution (497). The challenges in attribution and legal responsibility is also of concern for Simović, Rašević, and Simović (2020), who question “how to prove doubts about a state’s connection to hacker groups when an independent and impartial investigation can hardly be conducted in circumstances of growing tensions with a state labelled in advance as hostile” (32). When cyber operations cannot be conclusively attributed, it leaves states vulnerable to repeated attacks without the ability of holding perpetrators accountable, thereby losing their control over their own security. Chatinakrob (2024) adds that cyber threats, like state-sponsored attacks on critical infrastructure, undermine territorial control and stability, posing serious risks to sovereignty. He notes that while international law offers some ways to address these threats, enforcement is limited, and existing frameworks struggle to keep up with

technological changes (26). The lack of geographic boundaries in cyberspace, making it unable to "map neatly onto the traditional system of territorial jurisdiction," has also been noted by Perloff-Gilles (2018, 192). The idea of cyberspace sovereignty reflects the effort by states to assert control over digital infrastructure, but it is narrower than traditional territorial sovereignty and faces significant enforcement challenges (Chatinakrob 2024, 26). This shows that states are trying to adapt to new forms of interference while still holding onto their traditional authority.

Mueller (2020) offers a perspective that ties well into the arguments made by other scholars regarding the borderless nature of cyberspace. He takes a critical view of the concept of cyber sovereignty, arguing that attempts to apply traditional notions of sovereignty to cyberspace are inappropriate given the unique characteristics of the domain (780). Mueller emphasizes that cyberspace should be viewed as a global commons rather than a space subject to state sovereignty, as the technical architecture of the internet inherently undermines the concepts of territoriality and exclusive authority (780). His argument reinforces the challenges noted by Perloff-Gilles (2018) and Chatinakrob (2024), who point out the limitations of traditional jurisdiction and the narrower scope of digital sovereignty. Mueller's perspective thus challenges the applicability of the Westphalian model to cyberspace, suggesting that new governance models are needed to address the complexities of the digital age (780).

Paterson and Hanley (2020) put these challenges in the context of political warfare. They argue that the use of cyberspace by state and non-state actors to subvert democratic processes and interfere in elections represents a serious threat to the legitimacy of democratic states. The authors specifically mention the Russian interference in the 2016 US presidential election as an example of how foreign actors can leverage cyberspace to conduct political warfare aimed at undermining democratic governance (443). Such subversion is a great threat as it undermines the sovereignty and democratic principles of the target state. It challenges the values, beliefs, and independence of both the state and its citizens (442).

### 2.2 Continuity in Sovereignty: Arguments for Adaptation

Despite the challenges posed by globalization and cyber operations, several scholars argue that there is continuity in how sovereignty is maintained. Krasner (1999) offers an important perspective on the compromises and complexities of sovereignty in practice. He points out that while the Westphalian model emphasizes territorial autonomy and non-interference, in reality, sovereignty is often compromised and adjusted to meet practical needs. For example, states engage in international agreements and organizations that limit their

autonomy in exchange for economic or security benefits. Krasner suggests that these compromises do not mean sovereignty is obsolete but show its flexibility and adaptability to changing circumstances (117). This shows that sovereignty can change to meet new circumstances, rather than being completely undermined.

This perspective is perhaps also applicable in the context of cyber operations, where the concept of sovereignty could also adapt to new challenges, rather than being fundamentally undermined by them. The Tallinn Manual 2.0 (2017) provides a contemporary perspective on how traditional principles of sovereignty can be applied to the digital realm. The Tallinn Manual 2.0 is a comprehensive guide produced by an independent group of international law experts, aimed at understanding how international law, particularly the principle of sovereignty, applies to cyber operations. Originally commissioned by NATO's Cooperative Cyber Defence Centre of Excellence, the manual first focused on cyber operations involving the use of force and later expanded to cover peacetime operations as well (1-2). The Tallinn Manual 2.0 underscores that the principle of sovereignty remains foundational in cyberspace, asserting that states retain sovereignty over cyber infrastructure located within their territory and have the authority to regulate associated cyber activities (13). While cyberspace presents unique challenges due to its borderless nature, the manual argues that existing principles, such as territorial sovereignty and jurisdiction, continue to apply, though they may require nuanced adaptation to account for digital interactions (12).

The suggestion to turn cyberspace into a global commons, which has been put forward by Mueller (2020), because of its borderless nature, can be refuted by an argument put forward by Liaropoulos (2013). He points out that, in contrast to other global commons, cyberspace is not natural, but human-made, and it can therefore be unmade and regulated (21). Cyberspace needs physical infrastructure in order to operate and this infrastructure is located within the territories of states with laws (22). For these reasons he concludes that cyberspace is not immune to state sovereignty and that it is “a reflection of the current international system in a new domain” (23). Evidence for this conclusion can be found in real life examples. Authoritarian regimes are increasingly manipulating cyberspace to serve their strategic interests by employing both technical and legal measures to limit digital freedoms within their territories (Deibert 2015, 64). The implementation of these information controls has led to "a tightening grip on cyberspace within sovereign territorial boundaries," as states emphasize cybersecurity and anti-terrorism initiatives. Such restrictions are now normal, even in democracies (65). An increasing number of states are adopting rhetoric and practices that prioritize sovereignty over maintaining a free and open cyberspace (Schmitt and Vihul 2017, 218). This demonstrates that

states are still capable of asserting control over the digital realm in a manner similar to their authority over physical territory.

### 2.3 Conclusion of Literature Review

This literature review has revealed the division in academic literature regarding the impact of cyber operations on sovereignty. One perspective argues that cyber operations represent a fundamentally new challenge to traditional notions of sovereignty, particularly due to complexities like attribution, the involvement of non-state actors, and the borderless nature of cyberspace. This view suggests that traditional legal frameworks are insufficient, and new governance models may be required to address the unique characteristics of the digital domain. The other perspective highlights continuity in how sovereignty is exercised, asserting that existing international principles can adapt to the digital age. It is argued that while cyberspace presents challenges due to its borderless nature, states can still assert control over digital activities within their territories. Both authoritarian and democratic states have tightened their control over cyberspace, showing that the exercise of sovereignty has evolved rather than being undermined.

The aim of this thesis is to contribute to this ongoing debate by conducting a comparative analysis of CIA interference in Chile and Russian interference in the 2016 US presidential election. By examining these historical and contemporary cases of electoral interference, this research illustrates that violations of sovereignty, such as meddling in another state's domestic affairs, are not unique to the cyber era. Rather, they are a continuation of state behavior that predates digital technologies. The digital aspect does not fundamentally change the nature of such actions, and ultimately, sovereignty remains resilient even in the face of technological advancements. This research will contribute to the academic understanding of how cyber operations fit within the broader context of state sovereignty and international conduct, emphasizing the adaptive, rather than transformative, impact of these technologies.

## 3. Methodology

This chapter outlines the methodological approach used to answer the research question: “To what extent has state sovereignty evolved in the context of interstate cyber operations in peacetime, and how does it compare with interstate actions prior to the cyber era?” The research

draws on two comparative case studies of electoral interference, the CIA's involvement in Chile and Russian interference in the 2016 US elections, to assess whether cyber operations are a novel challenge to state sovereignty or merely a continuation of classic state behavior.

### 3.1 Theoretical Framework

This thesis adopts a realist theoretical framework to examine how states engage in electoral interference, both through traditional covert operations and modern cyber-enabled tactics. Rooted in the assumption that the international system is anarchic, realism posits that states act primarily out of self-interest, seeking to maximize their power and security while minimizing threats posed by rival actors (Korab-Karpowicz 2010, 4). The absence of a central authority in international politics compels states to rely on their own means to safeguard their interests, often leading them to interfere in the domestic affairs of others when doing so serves their strategic objectives (Mearsheimer 2001, 33).

Realism is particularly relevant to this study, as it offers a lens through which to analyze sovereignty and cyber operations within a framework that does not assume the primacy of legal norms but instead focuses on the pragmatic behavior of states. While some scholars, as discussed in the literature review of this thesis, argue that cyber operations represent a fundamental transformation in IR, realism suggests that, despite technological advancements, the motivations behind such operations remain consistent. The ability to influence foreign political environments without direct military confrontation is not a novel phenomenon, but rather a continuation of covert statecraft that has existed throughout history.

By applying realism, this thesis tests two key assumptions. Firstly, sovereignty should not be understood as an absolute or inviolable principle, but rather as a contested and adaptable concept. Realists such as Krasner (1999) argue that sovereignty has always been subject to violations and adjustments, as states routinely interfere in one another’s internal affairs when doing so aligns with their interests (8). Secondly, cyber operations should not be seen as a rupture in international politics, but rather as an evolution of long-standing state practices. From a realist perspective, the strategic logic of influence operations remains unchanged; only the tools have developed in response to new technological possibilities.

Although realism provides a strong foundation for understanding cyber interference, it is not without its limitations. One potential shortcoming lies in its state-centric focus, which may overlook the role of non-state actors such as independent hackers, private intelligence firms, or social media corporations in facilitating or resisting cyber operations. Furthermore, it

could be argued that the evolving nature of digital sovereignty, particularly in terms of legal and normative frameworks, such as the Tallinn Manual 2.0 (2017), calls for alternative theoretical approaches. Also the significance of technological shifts in cyber operations might be underplayed. This thesis accounts for this limitation by explicitly analyzing whether the technological tools used in election interference impact the effectiveness, scope, or strategic advantages of such operations. However, while these perspectives contribute to a broader discussion, realism remains the most suitable framework for this study because it centers on the state-driven nature of electoral interference and highlights the enduring logic of power politics.

This thesis will use realism as a guiding analytical lens in the comparative case study analysis. A key focus will be on the extent to which strategic self-interest motivated the US and Russia in their respective operations, and whether the objectives of electoral interference align with the pursuit of power as theorized by realism. Furthermore, attention will be given to how these states integrated their tactics into broader foreign policy strategies, reinforcing the idea that cyber operations are not an isolated or unique phenomenon but rather a continuation of historical state behavior. By adopting this framework, the thesis aims to demonstrate that cyber operations do not fundamentally alter the concept of sovereignty, but rather reaffirm the persistence of covert interference as a strategic tool in IR.

### 3.2 Comparative Case Study Approach

This study employs a qualitative comparative case study approach to examine two specific instances of electoral interference. Structured-focused comparison ensures that both case studies are examined using a common set of guiding questions, allowing for systematic analysis across different historical contexts (George and Bennett 2005, 67). These questions focus on identifying the primary tactics used, the intended target audiences, and how the strategies integrated into broader foreign policy objectives. The 'structured' aspect refers to the standardized set of guiding questions applied to both cases, ensuring that the same variables are assessed systematically. The 'focused' aspect means that the comparison is tailored to the research question, centering on the role of cyber operations and their implications for sovereignty (67). The comparison is designed to answer the following key questions for each case study:

- What were the strategic objectives behind the electoral interference?
- What tactics were used to influence political outcomes?
- Who were the target audiences, and how were they influenced?

- How was propaganda disseminated (traditional vs. digital methods)?
- How did the level of plausible deniability differ between the cases?
- What role did attribution play in shaping state responses?

The comparative nature of the analysis allows for an in-depth exploration of similarities and differences between two practices in different historical periods and contexts. The case study selection process began by determining the focus of this thesis, which is cyber operations during peacetime. When cyber operations are viewed as a component of warfare (i.e., cyber warfare), their implications for sovereignty are relatively straightforward: warfare inherently violate another state's sovereignty. However, the more pressing debate concerns whether cyber operations conducted outside the context of open conflict constitute a novel challenge to state sovereignty. This distinction is why this thesis refers to 'cyber operations during peacetime' rather than adopting the more popular but often misleading term 'cyber warfare'. The increased significance of cyber operations in contemporary IR stems largely from incidents such as the 2007 cyberattacks on Estonia and the release of the Stuxnet worm in 2010 (Zilincik and Duyvesteyn 2023, 840; Traynor 2007; Nakashima and Warrick 2012). The scholarly focus on the topic was further enhanced as a result of the 2016 Russian interference in the US elections, particularly regarding whether cyber operations mark a fundamental departure from historical state behavior (Paterson and Hanley 2020, 439).

While cases such as Estonia and Stuxnet played a foundational role in shaping the discourse on cyber warfare, they posed methodological challenges when attempting to identify suitable historical parallels. Stuxnet, for instance, was a US-Israeli cyber-sabotage operation targeting Iranian nuclear facilities to halt their nuclear development (Nakashima and Warrick 2012). The most apparent historical counterpart would be the Black Tom explosion of 1916, a case of German sabotage against US munitions supplies. At that time, the US was still neutral in World War I, but the Germans understood that the munitions were awaiting shipment to Europe to be used against them (Wills 2018). Hence, despite a formal peace between the US and Germany, there is still a significant wartime context. Additionally, the limited availability of both primary and secondary sources on the case are a further limitation. The challenge of finding pre-cyber counterexamples for cases like Stuxnet led to a reconsideration of the focus of this thesis. Electoral interference, by contrast, presented a more viable path for historical comparison, given the extensive record of states covertly manipulating foreign elections throughout the twentieth century.

The selection of electoral interference as the focal point of this study is not merely a matter of convenience, but is grounded in its analytical advantages. Unlike sabotage, where direct material consequences may distinguish cyber operations from their historical analogs, electoral interference is primarily an information-based activity. As such, it lends itself more naturally to a continuity-based analysis, where the role of emerging technologies can be evaluated without conflating the means of execution with the underlying strategic objectives. However, selecting an appropriate pre-cyber case study required further refinement. US electoral interference during the Cold War was widespread, particularly in Latin America. Yet many of these cases, such as US involvement in Nicaragua and El Salvador, were embedded within broader economic and military interventions, including the funding of rebel groups and military governments (Daghrir 2017, 88; Perla 2008, 145). These cases, while involving election manipulation, were part of larger, multifaceted interference campaigns that complicate direct comparison with modern cyber-enabled electoral interference.

Chile emerged as the optimal historical case due to the clarity of its objectives and the direct nature of US involvement. The CIA's actions in Chile were primarily aimed at influencing electoral outcomes through propaganda, targeted disinformation campaigns, and financial support for opposition groups, closely mirroring the methods used in Russian cyber operations in 2016. The absence of direct military intervention further aligns it with the peacetime parameters of this study.

### 3.3 Data Collection

This research relies on a combination of primary and secondary sources to examine the two case studies of electoral interference. The selection of sources was determined by the availability of declassified documents and the accessibility of reliable secondary literature. For the Chile case study, primary sources include declassified National Security Council (NSC) and CIA documents, which provide direct insight into US involvement in Chile. However, given the vast scope of available declassified material, secondary sources were also incorporated to contextualize and interpret these documents. A key source in this regard is Peter Kornbluh's *The Pinochet File: A Declassified Dossier on Atrocity and Accountability* (2013), which compiles a selection of declassified records related to US policy in Chile between 1970 and 1990. Kornbluh's work is particularly valuable because it is based on extensive archival research conducted at the National Security Archive, an organization directly involved in the declassification of US government documents. As a result, this book provides a comprehensive

and meticulously sourced account of CIA activities in Chile, offering structured access to primary materials that would otherwise require extensive archival research beyond the scope of this study.

In contrast, the Russian case study primarily draws on secondary sources. This difference in source availability arises from the fact that most critical details about Russian electoral interference in the 2016 US presidential election have been made public through official government investigations, most notably the *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (Mueller 2019). Unlike the Chile case, where declassified government documents provide direct insight into covert operations, the Russian case does not have a comparable collection of declassified material available for scholarly examination. While intelligence community assessments and investigative journalism contribute to the understanding of this case, significant limitations exist in accessing firsthand government documents due to ongoing classification policies. Given these constraints, the analysis relies on peer-reviewed academic studies and government reports that synthesize and interpret the available evidence.

The accessibility of sources inevitably influences the scope of research findings. Unlike intelligence analysts or government officials with access to classified materials, academic research is confined to publicly available declassified documents and secondary sources. However, this limitation does not significantly impact the validity of the conclusions drawn in this study. The sources currently available, whether through declassification efforts in the Chile case or through official investigations in the Russian case, offer a sufficiently complete picture for analyzing patterns of electoral interference. While future declassifications may provide additional details, the fundamental strategies and objectives of these operations are well-documented, allowing for a robust comparative analysis. On the other hand, a limitation that does potentially influence the research findings of this thesis is the sole use of Western sources, such as US government reports, declassified intelligence documents, and Western academic analyses. It is therefore shaped by the perspectives, biases, and framings inherent to these materials. The absence of Russian or Chilean primary sources, as well as non-Western interpretations of the case studies, may influence how the events are contextualized and understood. While these limitations do not invalidate the findings, they highlight the importance of recognizing potential gaps in perspective and the need for further research incorporating non-Western viewpoints

# 4. Comparative Analysis

This comparative analysis employs a structured-focused comparison to systematically assess whether cyber operations mark a fundamental shift in state behavior or a continuation of existing covert tactics. To maintain analytical consistency, the study applies a predefined set of questions to both case studies, covering strategic objectives, tactics, target audiences, media dissemination methods, geopolitical integration, sovereignty challenges, plausible deniability, and attribution issues. This approach ensures that each case is examined through a common lens, facilitating a precise evaluation of continuities and qualitative differences in electoral interference tactics over time. It will be shown in this chapter that the transition from traditional interference methods to modern cyber operations represent an evolution in state behavior, rather than a revolutionary change. Such continuity supports the broader argument that cyber operations are not an entirely new threat to state sovereignty, but rather a modern extension of longstanding practices. These case studies take place in different historical and geopolitical contexts. However, they share a common goal: to influence the political environment of target states while avoiding direct military confrontation.

## 4.1 Case Study: The CIA in Chile During the Cold War

The CIA's involvement in Chile must be understood within the broader context of US foreign policy during the Cold War, which was driven by a determination to prevent the global spread of communism. At the end of World War II in 1945, the US was aiming to transform the war-torn Europe into a bastion of democracy, free trade, and private enterprise that would align closely with American interests. An increasingly antagonistic Soviet Union, as well as the social and economic dislocation in many regions due to the war, challenged this vision (Callanan 2010, 10). The Administration of President Harry S. Truman quickly shifted from attempts at negotiation with the Russian leadership to viewing the Soviet Union as a potential enemy whose interests threatened the political and economic aims of the US and its allies (12). It is this context in which the CIA was born, and the fear of Soviet subversive capabilities caused the US leadership to conclude that the CIA needed similar capacities while avoiding the implications of exposure and accountability (Rudgers 2000, 250). The CIA was involved in a variety of operations, such as producing independent intelligence, conducting clandestine collections, and executing covert actions. However, up until 1948 these operations were restricted to employing a limited psychological warfare campaign to counter the political threat

from indigenous Communist Parties in Western Europe (Callanan 2010, 15). In the years after, due to a changing geopolitical environment, particularly in Asia, the US broadened its efforts to contain communism on a global scale. Concurrently, the CIA's covert action mission expanded to meet these growing policy demands (50). For the purpose of approving and supervising the covert activities conducted by the CIA and other intelligence agencies, the 40 committee was established in 1954 (initially as the 5412 committee). The committee's membership typically included the National Security Advisor (as chair), the Secretaries of State and Defense, the Chairman of the Joint Chiefs of Staff, and the Director of Central Intelligence. The 40 Committee ensured that covert actions aligned with US foreign policy objectives and maintained plausible deniability for the administration (Wise 1975). Also Latin America became subject to Cold War policies, as the Cuban Revolution sparked fear of a communist offensive in the region, threatening “continental unity and the democratic institutions of the hemisphere” (Harmer 2019, 114). The CIA had missions in several Latin American countries, of which this study will focus on the agency’s effort to undermine communism in Chile.

CIA covert actions in Chile had started in 1962. The main goal, deeply embedded in the Cold War policies of the time, was to undermine Marxist-leaning political figures, particularly Dr. Salvador Allende, and to bolster and support their civilian and military adversaries to prevent them from gaining power. The operation began with financial aid to the Christian Democratic Party (PDC) to support the 1964 Presidential candidacy of Eduardo Frei against Allende’s Unidad Popular (UP) party. Over time, the covert actions evolved into a multi-million dollar campaign, intensifying when Allende was elected in 1970 as the new Chilean president (CIA 2000). The US intervention in Chile against the presidency of Allende is a significant example of covert action to affect political outcomes by using propaganda, disinformation, and economic manipulation. This case study examines the role of the CIA in support of anti-Allende efforts, focusing on the agency's use of propaganda to destabilize Allende's government and create an atmosphere favorable for a coup.

The CIA's covert campaign against Allende involved fostering what has been described as a "coup climate" in Chile. The objective was to destabilize the political environment, thereby making military intervention seem justifiable. Propaganda, disinformation, and psychological warfare were used to achieve this, including spreading false reports and initiating terrorist activities to provoke an anti-government reaction (Kornbluh 2013, 14; 20). The propaganda efforts aimed to portray Allende's government as a threat to Chilean stability and to heighten public tension, thereby weakening support for Allende (87). One of the major strategies employed by the CIA included using the media to manipulate public perception. The agency

covertly funded *El Mercurio*, Chile's largest right-wing newspaper, to put pressure on Allende's government. Declassified NSC documents regarding 40 committee meetings reveal that *El Mercurio* requested a $1 million funding from the US in 1971, so that it could survive the economic squeeze it has been undergoing as a result of increasing governmental control over finance and businesses in Chile (NSC 1971, 1). The funding would prevent Allende from shutting down the newspaper, as it would be a major freedom of press issue. Without this support, Allende could allocate the closing of *El Mercurio* to its financial ineptitude (2). A declassified CIA document confirms that $1 million was indeed passed to *El Mercurio* and that it since has been publishing almost daily editorials aimed against Allende (CIA 1973, 3). In 1972, an additional funding of $1 million was proposed by the CIA, which stressed the importance of *El Mercurio* (NSC 1972, 2). The newspaper consequently played a key role in shaping public opinion by spreading fear and portraying Allende as a threat to Chilean democracy. Articles and editorials published in *El Mercurio* were intended to create dissatisfaction and incite public agitation, which would eventually lead to a coup (Kornbluh 2013, 92; Morley and Smith 1977, 213). This propaganda extended to radio broadcasts and other forms of media, reaching a broad audience, particularly the working class (Gustafson 2007, 70). The propaganda campaign also involved sophisticated use of selective framing, as *El Mercurio* employed the "selective and framed use of international news" to create a moral panic, presenting international events in a way that linked Allende's government to the broader threat of communism (Alvear and Lugo-Ocando 2018, 529).

The CIA also utilized economic propaganda as a destabilization tactic, promoting rumors of economic collapse to induce panic among the Chilean population. For instance, propaganda campaigns falsely suggested that international companies were ceasing operations in Chile, and rumors were spread about imminent food shortages. Such disinformation campaigns were intended to undermine public confidence in Allende's ability to govern and to induce social unrest (Kornbluh 2013, 18; Kim 2005, 41). *El Mercurio* played a significant role in this economic destabilization by announcing artificial shortages, such as detergent shortages, which prompted panic-buying and created artificial economic crises, fueling dissatisfaction with Allende's government (Kim 2005, 41). The CIA also subsidized other newspapers, magazines, and radio stations, effectively creating a coordinated media network that supported US goals in Chile (Morley and Smith 1977, 213). The campaign aimed to portray Allende's leadership as chaotic and incapable of managing the country, thereby justifying the need for a change in leadership.

In addition to propaganda through the media, the CIA poured substantial resources into funding opposition groups and mobilizing anti-Allende political forces. A report by the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (Church Committee) reveals that $8 million was allocated to the propaganda for elections and other support for political parties between 1963-73 (Church Committee 1975, 7). Key political figures were mobilized by the CIA, including Eduardo Frei, who had served as the president before Allende. The agency created fictitious telegrams from women's groups, purportedly coming from other Latin American countries, urging Frei's wife to take action against Allende (Kornbluh 2013, 13). This effort was part of a broader campaign to create an anti-Allende consensus among influential figures in Chile, ensuring that political opposition to Allende remained strong and vocal. The use of gendered propaganda was also evident in the CIA's "Scare Campaign," which specifically targeted women by portraying a communist victory as an existential threat to the family and motherhood, thereby aiming to sway female voters against Allende (Power 2008, 941). The CIA's support also extended to funding strikes and demonstrations, such as the truckers' strike, which significantly disrupted Chile's supply chains and contributed to a climate of chaos and instability (Morley and Smith 1977, 213). These strikes were portrayed in the media as spontaneous uprisings against Allende, reinforcing the narrative that his government was losing control.

The US psychological warfare campaign in Chile was multifaceted, involving direct propaganda through the media as well as more subtle psychological operations. The CIA coordinated propaganda across different media outlets to maximize its impact. This campaign sought to influence public perception by framing Allende's government as chaotic and linked to communism, a narrative that resonated with fears of instability and the spread of communism during the Cold War era (Landis 1975, 213; Alvear and Lugo-Ocando 2018, 530). *El Mercurio* was central to this psychological warfare, portraying Allende's government as responsible for "chaos and anarchy" and creating associations between Allende and the Soviet Union. Headlines were often misleading, paired with unrelated but striking images to evoke fear and uncertainty among readers (Landis 1975, 225). This propaganda helped mobilize public sentiment against Allende, particularly targeting the middle class by emphasizing the supposed threat to Chilean democracy posed by a socialist government (Alvear and Lugo-Ocando 2018, 530-534).

The Chile case illustrates the extensive use of propaganda and covert funding by the CIA to influence political conditions abroad without revealing direct US involvement. By leveraging media outlets such as *El Mercurio*, spreading disinformation about economic

conditions, and coordinating with political actors to influence public sentiment, the CIA created a favorable environment for the eventual military coup against Allende. This case exemplifies the continuity in tactics of covert intervention, similar to how modern state actors utilize cyber operations today to achieve comparable goals of political destabilization.

### 4.2 Case Study: Russian Interference in the 2016 US Elections

The Russian interference in the 2016 US presidential election did not occur in a vacuum. Instead, a variety of factors was at play, including geopolitical tensions, Russian President Vladimir Putin's desire to destabilize the US, and to boost presidential candidate Donald Trump's campaign. This is best seen as a continuation of broader strategic objectives aimed at reasserting its influence and challenging perceived threats from Western institutions. Since the collapse of the Soviet Union, Russia has perceived itself as marginalized by Western powers, whose continued influence in Eastern Europe, particularly through the eastward expansion of the North Atlantic Treaty Organization (NATO) and the European Union (EU), has been seen as a direct threat to Russian national security (Galeotti 2019, 31). Other issues, such as the Kosovo crisis in 1998/99, the Russo-Georgian War in 2008 and the Russo-Ukrainian War that began in 2014, have further illustrated the sharp dissonance between Russian and Western perceptions of international affairs (Monaghan 2016, 1-2). Putin had also pointed his finger at Hillary Clinton in 2011 for allegedly encouraging mass protests in Moscow by issuing a statement that recent elections, in which Putin aimed for a third term, were rigged (Jamieson 2020, 22). When Clinton faced Trump in the 2016 presidential election, it is for this reason that Putin was more in favor of the latter, who was perceived to be more friendly towards Russia and its policies (Jones 2019, 6). This context set the stage for Russia to interfere in the elections.

The Russian interference in the 2016 US presidential election was a complex campaign with multiple dimensions that sought to influence American political outcomes. Putin is reported to have personally ordered an influence campaign aimed at undermining public faith in the US democratic process, damaging Clinton's candidacy, and supporting Trump (Van Atta 2018, 2). This campaign blended cyber operations and propaganda, marking an extraordinary effort by a foreign state to interfere in a US election through psychological and digital tools. It has been reported that on Facebook alone 126 million Americans have been exposed Russian cyber operations between 2015 and 2017 (Vićić and Gartzke 2024, 14). The primary objectives were not only to promote specific candidates but also to create lasting divisions within American society, weakening the country from within (14).

Russian interference relied heavily on digital platforms such as Facebook, Twitter, and Google. Through the Internet Research Agency (IRA), Russia orchestrated an extensive social media campaign designed to influence voter opinion and increase social divisions (McCombie, Uhlmann, and Morrison 2020, 98). The IRA was founded in 2013 in St Petersburg by a close ally to Putin with links to Russian intelligence (Scott 2020, 76). The notorious Yevgeny Prigozhin, founder of the Russian private military company Wagner, admitted years later that he was behind the IRA (Krever and Chernova 2023). Fake accounts and bots distributed disinformation that targeted Clinton while promoting Trump. The IRA's "troll farms", a coordinated group formed specifically to influence public opinion by creating and spreading false or misleading information online, spread divisive content across multiple platforms, employing organized groups to influence public opinion by disseminating misinformation. These trolls used fictitious social media personas to emphasize existing social conflicts and manipulate voter behavior (McCombie, Uhlmann, and Morrison 2020, 97). With each troll being "expected to post 50 news articles daily and maintain six Facebook and 10 Twitter accounts, with 50 tweets per day", it became difficult for the mainstream media to distinguish trolls from real accounts (Ajir and Vailliant 2018, 76). Facebook initially denied that its platform had been used to spread anti-Clinton propaganda, but they eventually admitted "that it had removed hundreds of fake accounts that attacked Clinton, or spread divisive disinformation, which were linked to Russian intelligence services, and that Facebook had sold at least $100,000 worth of anti-Clinton ads to Russian sources" (Kellner 2018, 145). However, of this amount only 46% was spent prior to the election and the remainder after. In comparison, Trump and Clinton had spent $81 million on Facebook ads in their campaigns (Select Committee on Intelligence 2017, 76). That this relatively small investment by the IRA could have such an impact on the confidence in the US electoral system showcases the efficiency of the IRA.

Online ads were a key aspect of the Russian influence operations. It targeted specific demographic groups, particularly African Americans, who were perceived to be vulnerable to divisive messaging due to ongoing racial tensions in the US. Ads aimed at African Americans highlighted themes such as police brutality and systemic injustice, drawing on older Soviet-era tactics of exploiting societal cleavages to destabilize adversary states (Vićić and Gartzke 2024, 20-21). The campaign also employed a three-phase strategy known as Identification-Imitation-Amplification (IIA), which involved identifying target groups based on their online behavior, imitating authentic conversations, and amplifying these messages through bots to create echo chambers (14). This approach heightened divisions among targeted groups and reinforced existing biases, particularly regarding issues like race and gun rights (15). By utilizing such

topics the Russian campaign provoked strong reactions and discouraged voter turnout. A method used by the IRA was creating fictitious organizations that were specifically designed to spread content aimed at influencing certain groups. For instance, the "Blacktivist" organization focused on issues like police brutality, aiming to mobilize support, discourage voting, and influence perceptions within African American communities (McCombie, Uhlmann, and Morrison 2020, 99). The use of emotionally charged narratives was meant to sow discord and ultimately discourage participation among voters less favorable to Trump. Interestingly, much of the content shared by Russian actors was not entirely false. Instead, they used factually correct information framed in ways that exacerbated social divisions. By emphasizing genuine grievances, the Russians shaped public discourse to create distrust in the democratic community. The majority of the ads (94.42%) used accurate information, but framed it in such a way that it highlighted societal conflicts and deepened divisions (Vićić and Gartzke 2024, 18).

Russian state-funded media outlets like RT (formerly Russia Today) and Sputnik, which maintain offices in various Western countries, also played a role in amplifying disinformation (Inkster 2016, 28). These outlets broadcasted propaganda in English and other languages that challenged the impartiality of Western media, frequently portraying Clinton negatively while supporting Trump. Their strategy relied on emotionally appealing content that could be widely shared on social media, thereby increasing its reach (Scott 2020, 76). Popular English-language videos by RT, such as "Trump Will Not Be Allowed to Win" and "How 100% of the Clintons' Charity Went to... Themselves," were widely shared on social media, garnering millions of views. Fueled by passion and bias, people are vulnerable to this kind of fake news and other disinformation because these exaggerated or false claims often match their political beliefs (76).

Besides funding the propaganda campaign, media reports have also speculated about Trump's electoral campaign receiving funds from Russian sources. There is no official evidence that Russia directly funded Trump's 2016 campaign. However, the reports are noteworthy for the sake of this comparative analysis. As reported by *The Guardian*, Russian-American businessman Simon Kukes made significant donations to Trump's campaign and associated political committees in 2016. Kukes, who had previously led a Russian state-owned oil company, contributed over $273,000 during the election cycle. Notably, these were his first recorded political donations, and they coincided with his communications about active involvement in Trump's campaign. These revelations have raised questions about the origins and motivations behind his contributions (Harding 2018). Another report comes from *McClatchy.* The Federal Bureau of Investigation (FBI) investigated whether Russian banker Alexander Torshin funneled money through the National Rifle Association (NRA) to support

Trump's campaign. Torshin, a deputy governor of Russia's central bank with close ties to both President Vladimir Putin and the NRA, was suspected of directing funds to the organization, which then significantly increased its spending to back Trump in 2016. While the NRA reported substantial expenditures in support of Trump's candidacy, the investigation sought to determine if any of these funds originated from Russian sources, which would violate US campaign finance laws prohibiting foreign contributions (Stone and Gordon 2018). And finally, *The New York Times* reveals that Viktor Vekselberg, a Russian oligarch with close ties to the Kremlin, was found to have directed payments to Michael Cohen, Trump's personal attorney. In 2017, entities associated with Vekselberg's conglomerate, Renova Group, paid Cohen's consulting firm substantial sums. While these payments occurred after the election, they have been scrutinized for potential connections to Russian efforts to gain influence within Trump's inner circle (Rashbaum, Protess, and McIntire 2018). These instances, reported by reputable media outlets, underscore the complex web of interactions between Trump associates and Russian-linked individuals, although definitive evidence of direct Russian funding to Trump's 2016 campaign has not been established.

The extensive propaganda campaign and potential funding of Trump's election campaign was combined with cyber-attacks, such as the hacking of the Democratic National Committee (DNC) and the Democratic Congressional Campaign Committee (DCCC) and the subsequent release of emails via platforms like WikiLeaks. According to a US Department of Justice (DOJ) report by Mueller, the Russian military intelligence service (GRU) hacked the DNC and DCCC networks, stealing hundreds of thousands of documents. The GRU published these documents through fictitious online personas like "Guccifer 2.0" and "DCLeaks" (Mueller 2019, 36). The release of this information was strategically timed, with WikiLeaks publishing the first batch on July 22, 2016, just as the Democratic National Convention was starting (46). Another major release came on October 7, 2016, less than an hour after the "Access Hollywood" tape was leaked. This also appears to be a deliberate timing to sway away attention from the Trump scandal towards Clinton (58). The emails revealed a bias within the DNC in favor of Clinton over Bernie Sanders, which led to the resignation of DNC chairperson Debbie Wasserman Schultz. The leaks, while not providing evidence of significant wrongdoing, were damaging to the credibility of the DNC and fueled public skepticism, further enhancing the effect of the Russian disinformation campaign (Inkster 2016, 23).

It has also been reported that Russian intelligence gained access to multiple state or local electoral boards. However, the type of systems that were targeted had no involvement in vote tallying (ODNI 2017, 3). Therefore, it can reasonably be assumed that the vote tallying process

remained unaffected by Russian cyber operations during the 2016 US elections. The breach did result in the extraction of personal information of US voters and the Russians had the ability to manipulate this data, but there were no indications that had been the case (SSCI 2019, 22). Why they did not do so remains an open-ended question. Potentially this fitted in the larger plan of undermining confidence in the US electoral system by showcasing their capabilities (23).

Besides the hack on the electoral boards not having an impact on the election outcome, there are also indications that the direct effect of the IRA campaign on voting behavior was minimal. Yet, the broader objective of sowing discord and eroding confidence in democratic institutions was largely successful. Russian actors exploited Trump's surprise victory to exaggerate the perceived impact of their intervention, further undermining confidence in the legitimacy of the election (McCombie, Uhlmann, and Morrison 2020, 95). The effectiveness of these tactics can be seen in the resulting environment of mistrust and division. Troll campaigns, social media ads, and propaganda broadcasts succeeded in reinforcing biases and keeping polarizing narratives at the forefront of public discussion throughout the election cycle.

In conclusion, the Russian interference in the 2016 US election was a sophisticated cyber operation containing a blend influence operations, propaganda dissemination, and hacking designed to influence political outcomes. By leveraging online news outlets, social media platforms, and cyber-attacks on Democratic institutions and electoral boards, Russia was able to introduce significant doubt into the US democratic process and influence public perceptions in a manner that continues to have repercussions today.

### 4.3 Comparative Analysis: Parallels and Differences Between Covert Influence Operations

This comparative analysis applies a structured-focused comparison to systematically evaluate the similarities and differences between CIA electoral interference in Chile and Russian interference in the 2016 US elections. By employing a standardized set of analytical questions, this section ensures that both cases are examined through a consistent lens, facilitating an evaluation of whether cyber operations represent a fundamental shift in state behavior or an evolution of pre-existing covert tactics.

#### 4.3.1 Strategic Objectives Behind Electoral Interference

Both the CIA and Russian intelligence sought to manipulate electoral outcomes to serve their respective geopolitical interests. During the Cold War, the CIA's primary objective in Chile was to prevent the consolidation of a Marxist government under Allende, a leader perceived as

a potential Soviet ally. This operation was part of the broader US strategy of containment, aiming to curb the spread of communism in Latin America and maintain regional stability under pro-Western regimes. Similarly, Russian interference in the 2016 US elections was motivated by strategic interests, albeit in a different context. The Kremlin sought to weaken the US political system, deepen societal divisions, and favor a candidate who was perceived as more accommodating to Russian interests. Putin's personal hostility toward Clinton, whom he blamed for supporting anti-government protests in Moscow in 2011, further reinforced Russia's incentive to intervene. From a realist perspective, both cases illustrate the state's intent of survival. In both cases, the state who is interfering in another state's elections is acting out of the perception of being under threat. The US saw the Marxist Allende as a direct threat to it's hegemony in the Western hemisphere, while Putin observed the eastward expansion of NATO and the EU as threatening to his state's survival. Hence, both countries meddled in the elections of their target states to force a favorable result.

### 4.3.2 Tactics Used to Influence Political Outcomes

Despite operating in different historical contexts, both covert actions employed propaganda, disinformation, and psychological warfare to influence public perception. In Chile, the CIA worked through traditional media channels, most notably by funding *El Mercurio*, the country's largest right-wing newspaper, to disseminate anti-Allende narratives. This strategy extended beyond print media, incorporating radio broadcasts and direct funding of opposition groups to organize protests and labor strikes. By portraying Allende's government as economically incompetent and ideologically extreme, the CIA sought to generate public disillusionment and increase pressure for regime change.

In contrast, Russian intelligence exploited digital media ecosystems to achieve similar goals. The IRA, a state-backed organization, coordinated a vast network of fake social media accounts designed to amplify politically polarizing content. Russian operatives produced and promoted divisive narratives, spreading disinformation that undermined trust in the electoral system and discouraged voter participation, particularly among key demographic groups. The hacking of the DNC and the DCCC further escalated the impact of the operation. Leaked emails, strategically released via WikiLeaks, aimed to damage Clinton's credibility, mirroring historical tactics used to discredit political adversaries.

While the core methods of propaganda and disinformation remained consistent across both cases, the introduction of cyber tools in 2016 allowed Russia to achieve greater scale, speed, and deniability than was possible in Cold War era interventions.

### 4.3.3 Target Audiences and Influence Strategies

Both covert operations strategically identified and targeted key societal groups whose political behavior could be influenced. From a realist perspective, this is seen as weakening adversary states from within. In Chile, the CIA focused its efforts on the middle class, business elites, and opposition politicians, recognizing that economic instability and ideological fears could drive them away from Allende. Additionally, gendered propaganda played a crucial role, as women were targeted with messages suggesting that a socialist government would threaten traditional family structures and national stability. Economic sabotage was also used as a means of persuasion, as rumors of food shortages and financial collapse were deliberately spread to weaken public confidence in the government.

The Russian interference campaign, by contrast, adopted a more granular, data-driven approach to audience targeting. Social media algorithms enabled operatives to deliver customized messages to different demographic groups, tailoring content to exploit existing social and racial tensions. African American voters, for example, were targeted with narratives emphasizing police brutality and systemic injustice, discouraging their participation in the election. Unlike the Chile case, where propaganda efforts were largely centralized through mainstream media, the Russian operation capitalized on decentralized, user-driven engagement, making disinformation appear more organic and credible.

### 4.3.4 Media Dissemination: Traditional vs. Digital Tools

A crucial distinction between these cases lies in how propaganda was disseminated. The CIA relied on print newspapers, radio broadcasts, and financial backing for opposition media, ensuring that anti-Allende narratives reached a broad audience through traditional means. The success of this strategy depended on controlling influential news outlets and generating a sustained information campaign.

Conversely, the Russian operation leveraged social media as its primary tool, enabling direct, real-time interaction with audiences in ways that traditional media could not (Paterson and Hanley 2020, 440). Additionally, the use of automated bots and coordinated troll networks allowed Russia to artificially amplify certain narratives, making them appear more widespread than they actually were.

While both cases demonstrate the strategic importance of media in electoral interference, the shift from traditional news control to algorithm-driven digital engagement represents a significant evolution in covert influence tactics.

### 4.3.5 Plausible Deniability and Attribution Challenges

One of the most striking differences between Cold War era covert actions and modern cyber operations is the issue of attribution. The CIA's activities in Chile, while initially covert, were later exposed through declassified government documents and congressional investigations. Despite efforts to maintain secrecy, the tangible nature of these operations, such as direct financial transfers to media outlets and political groups, ultimately left a paper trail.

In contrast, Russia's 2016 operation exploited cyberspace's inherent anonymity to maintain plausible deniability. By using private entities such as the IRA and hacking groups with no formal state affiliation, the Kremlin could obscure its direct involvement. Even when Western intelligence agencies identified Russian fingerprints in the election interference, Moscow dismissed the accusations as baseless, leveraging the difficulty of proving cyber attributions with absolute certainty.

This attribution problem is one of the most consequential developments in modern electoral interference. While Cold War era operations eventually became public knowledge, cyber-enabled interventions introduce new layers of uncertainty, allowing states to engage in covert influence with reduced accountability.

Here, realism helps explain why states prefer covert operations over direct confrontations. Given the costs of open warfare or diplomatic backlash, states will engage in influence operations that offer maximum strategic gain with minimal risk. Cyber operations enhance plausible deniability, but do not fundamentally alter the cost-benefit logic of covert action that has existed for decades.

### 4.3.6 Sovereignty Challenges: Evolution or Adaptation?

Both cases represent violations of sovereignty, but the nature of these violations has evolved. The CIA's intervention in Chile involved direct financial and logistical support to opposition groups, aligning with a traditional understanding of foreign interference. Russia's interference, however, blurred the boundaries between state action and digital subversion, operating in the gray zone of cyber-enabled covert influence.

This distinction suggests that sovereignty is not being fundamentally eroded but is instead adapting to new technological realities. While the digital realm complicates enforcement and attribution, states continue to exercise sovereignty by developing cyber defenses, regulatory measures, and counter-disinformation strategies to protect electoral integrity.

# 5. Discussion

The purpose of this chapter is to bring together the findings of this research, establish connections to the literature review, discuss the implications of the analysis, and address the central research question: "To what extent has state sovereignty evolved in the context of interstate cyber operations in peacetime, and how does it compare with interstate actions prior to the cyber era?" By employing a structured-focused comparison, this study has systematically evaluated two cases of electoral interference across a common set of analytical dimensions. The findings reveal both significant continuities in strategic intent and notable qualitative differences in implementation, particularly in the areas of plausible deniability and attribution. The use of cyber tools in the 2016 case did not introduce fundamentally new objectives but rather enhanced the scale, efficiency, and obfuscation of traditional influence tactics. This confirms that while cyber operations have modernized state behavior, they do not constitute a radical departure from historical sovereignty violations.

## 5.1 Revisiting the Research Question

The findings of this thesis suggest that interstate cyber operations during peacetime, such as Russian election interference in 2016, are not a fundamentally new threat to state sovereignty. Instead, they represent a modern extension of long-standing practices in statecraft, specifically in covert influence operations. The Westphalian model, which highlights territorial control, free from external interference, is undoubtedly undermined by such cyber operations. However, the similarity in operations, when comparing it to how the CIA operated in Chile during the Cold War, illustrates that the cyber dimension is merely a modern tool, while the strategic intent and objectives remain consistent. To provide an answer to the research question of this thesis, it can therefore be concluded that the emergence of cyber operations have not caused the concept of state sovereignty to evolve.

The realist theoretical framework underpinning this research provides a compelling lens through which to view the persistence of these tactics. Realism posits that states inherently act to maximize power and security, and cyber operations fit neatly within this broader pursuit. Whether it was the CIA's covert funding of opposition media in Chile or Russia's deployment of digital propaganda through troll farms, the underlying goal has been to manipulate political environments in favor of the interfering state's interests. The analysis suggests that sovereignty,

far from being obsolete, remains resilient, though it must continuously adapt to new challenges presented by technological advancements.

### 5.2 Connecting to the Literature Review

The discussion of cyber operations as a continuation of historical state behavior resonates strongly with the perspectives explored in the literature review. The arguments put forth by Krasner (1999) regarding the flexibility and adaptability of sovereignty are particularly relevant here. Krasner's notion that sovereignty is often compromised in practice, yet remains a fundamental organizing principle, aligns with the thesis' findings that state sovereignty has adapted to cyber challenges rather than being fundamentally undermined.

The literature review explored divergent views on the impact of cyber operations on sovereignty, with scholars like Mueller (2020) arguing for a fundamental rethinking of sovereignty in the digital age, while others, such as Liaropoulos (2013), emphasized the continuity of state control over digital infrastructure. The Tallinn Manual 2.0 (2017) stresses the nature of international law, in which covert actions are arguably already prohibited (Berkeley La Raza Law Journal 1984, 139). Since cyber operations are generally covert, there is no need for a fundamentally new legal framework to reconceptualize sovereignty. The analysis of the two case studies has visualized the similarities between a modern cyber operation and a pre-cyber covert action. This supports the argument that the concept of sovereignty has not significantly evolved, but is rather undergoing adaptation to cyberspace.

### 5.3 Implications for Sovereignty and International Law

The findings of this research carry notable implications for how state sovereignty is conceptualized and operationalized in the digital age. Despite the emergence of cyberspace as a new domain for state action, the persistence of covert interference tactics underscores that sovereignty remains a central organizing principle of the international system. However, the tools used to assert or undermine sovereignty have evolved, necessitating adjustments in how sovereignty is defended and exercised. As Krasner (1999) and the Tallinn Manual 2.0 suggest, sovereignty is adaptable, and this adaptability highlights the need for international law to keep pace with technological innovations.

A key challenge posed by cyber operations is attribution. Unlike traditional forms of interference, where actors and actions are often more readily identifiable, the digital nature of cyber operations allows for plausible deniability. This complicates the enforcement of

accountability under existing international legal frameworks, as highlighted by Mueller (2020) and Chatinakrob (2024). The difficulty in directly linking cyber interference to specific actors raises important questions about the adequacy of current legal mechanisms and whether new frameworks are needed to address this gap. Without clear attribution, holding states accountable becomes a significant hurdle, weakening the deterrent effect of international law. Moreover, the findings suggest that states are not only leveraging cyberspace to exert influence but are also increasingly vulnerable to similar actions from other actors. This dual dynamic underscores the interconnectedness of the digital realm, where offensive capabilities must be balanced with robust defensive measures. The emphasis on cybersecurity, as discussed by Deibert (2015), reflects a broader trend among states to tighten control over digital infrastructure within their territories. This assertion of digital sovereignty mirrors traditional practices of physical territorial control, highlighting the continuous adaptation of sovereignty to new technological and geopolitical realities.

Ultimately, these findings reinforce the enduring relevance of sovereignty in an era characterized by rapid technological change, while also pointing to the urgent need for international law to evolve. By addressing the challenges of attribution and the balance between offensive and defensive strategies, states can better navigate the complexities of cyber operations and uphold the principles of sovereignty in the digital age.

### 5.4 Limitations and Avenues for Future Research

The scope of this study is limited by its focus on two case studies of electoral interference. While this focus allows for a detailed comparison, it may not fully capture all dimensions of interstate cyber operations or the broader spectrum of covert interference tactics. Other noteworthy cyber operations, such as the 2007 cyber-attacks against Estonia (Traynor 2007) or the release of the Stuxnet computer worm on Iranian nuclear facilities in 2010 (Nakashima and Warrick 2012), still offer the possibility for a comparative analysis with similar historical accounts of sabotage to determine a potential continuity in state behavior. However, it must be noted that similar approaches to examining cyber operations have been explored in existing research. For instance, Lennart Maschmeyer (2024) wrote a book in which he extensively compares a case of cyber-enabled subversion, though not during peacetime, with a traditional form of subversion. His work, similar to this thesis, portrays the cyberspace as a tool for state behavior, rather than a fundamental threat to it. It therefore supports the argument of this thesis. What distinguishes this thesis is its focus on the impact of cyber operations on the

concept of sovereignty, with an emphasis on peacetime operations. This scope is crucial, as the concept of sovereignty is inherently compromised during wartime, making it more challenging to assess the continuity of state behavior without such a context.

Future research could also explore the implications of cyber operations for smaller states and non-state actors. While this thesis focused on major powers, such as the US and Russia, the impact of cyber operations on smaller states with limited cybersecurity capabilities warrants further investigation. Additionally, the role of non-state actors, including private companies and hacktivist groups, in shaping the landscape of cyber operations presents an important area for future study.

## 6. Conclusion

This thesis has examined the extent to which state sovereignty has evolved in the context of interstate cyber operations in peacetime, focusing on the comparative analysis of CIA electoral interference in Chile and Russian interference in the 2016 US elections. The findings demonstrate that while cyber operations introduce new tools and methods, the strategic objectives of covert interference have remained consistent. Both historical and modern cases reveal a continuity in state behavior, where sovereignty is challenged through indirect means to achieve geopolitical goals without direct confrontation. However, the role of cyber tools in modern operations has created new dimensions of plausible deniability, scalability, and attribution difficulties, distinguishing them from their pre-digital predecessors.

The comparison highlights that digital platforms and cyber-attacks serve as contemporary extensions of traditional methods such as media manipulation and economic destabilization. Yet, cyber operations allow for greater immediacy, reach, and automation, enabling actors to influence foreign political environments at an unprecedented scale. These qualitative differences underscore how technology has enhanced the efficiency and obfuscation of interference rather than fundamentally transforming state behavior.

From a realist perspective, this continuity is unsurprising. States have always sought to maximize their power and security through covert means, adjusting their methods to technological advancements. The cases of Chile and the 2016 US election exemplify how electoral interference remains a strategic tool of statecraft, adapted to contemporary information ecosystems. The findings of this research thus reinforce the notion that sovereignty remains resilient despite evolving forms of interference. While the digital realm complicates

enforcement and accountability, states continue to assert sovereignty by developing cyber defenses, regulatory measures, and counter-disinformation strategies.

Nevertheless, the implications for sovereignty and international law are significant. The difficulty of attribution in cyber operations complicates the enforcement of legal frameworks, raising questions about accountability and deterrence. Unlike traditional covert actions, where material evidence often surfaced, cyber operations introduce layers of ambiguity that enable perpetrators to evade direct responsibility. This gap necessitates further development in international legal mechanisms to address the evolving nature of cyber interference.

While this study provides a foundational comparison, future research should explore additional cases beyond electoral interference to assess the broader impact of cyber operations on sovereignty. Investigating cyber-enabled sabotage, economic manipulation, or hybrid warfare strategies could offer deeper insights into how states wield digital tools across different domains. Additionally, examining the responses of targeted states, whether through countermeasures, legal frameworks, or diplomatic strategies, would provide a more comprehensive understanding of how sovereignty is defended in the digital age.

Ultimately, this thesis demonstrates that cyber operations do not necessitate a fundamental redefinition of sovereignty but rather highlight its adaptability. As states continue to navigate the challenges of the cyber era, the principles of sovereignty endure, evolving alongside the technologies that shape interstate competition and influence.

## Bibliography

"Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Edited by Michael N. Schmitt, 2nd ed., Cambridge University Press, 2017. https://doi.org/10.1017/9781316822524.

Afyare, Abdifatah Ahmed Ali. 2024. "The Impact of Globalization on State Sovereignty." *International Journal of Science and Research Archive* 12 (2): 1653–62. https://doi.org/10.30574/ijsra.2024.12.2.1434.

Ajir, Media, and Bethany Vailliant. 2018. "Russian Information Warfare: Implications for Deterrence Theory." *Strategic Studies Quarterly : SSQ* 12 (3): 70–89. https://www.jstor.org/stable/26481910.

Alvear, Francisco Javier, and Jairo Lugo-Ocando. 2018. "When Geopolitics Becomes Moral Panic: *El Mercurio* and the Use of International News as Propaganda against Salvador Allende's Chile (1970–1973)." *Media History* 24 (3–4): 528–46. https://doi.org/10.1080/13688804.2016.1211929.

BBC. 2018. "Trump Sides with Russia against FBI at Helsinki Summit," July 16, 2018. https://www.bbc.com/news/world-europe-44852812. Accessed January 30, 2025.

Beal, Vangie. 2024. "Cyberspace." Techopedia. September 23, 2024. https://www.techopedia.com/definition/2493/cyberspace. Accessed December 6, 2024.

Beaulac, Stephane. 2020. "The Westphalian Model in Defining International Law: Challenging the Myth." *Australian Journal of Legal History* 8 (2): 181–213. https://doi.org/10.3316/informit.345957784564165.

Berkeley La Raza Law Journal. 1984. "Legality of Covert Action under Contemporary International Law." https://doi.org/10.15779/Z38GD3N.

Bodin, Jean. 1955. *Six Books of the Commonwealth*. Translated by M.J. Tooley. Abridged and Translated edition. Basil Blackwell. https://www.yorku.ca/comninel/courses/3020pdf/six_books.pdf.

Callanan, James. 2010. *Covert Action in the Cold War: US Policy, Intelligence and CIA Operations*. First Edition. London: I.B.Tauris. https://doi.org/10.5040/9780755625208.

Chatinakrob, Thanapat. 2024. "Interplay of International Law and Cyberspace: State Sovereignty Violation, Extraterritorial Effects, and the Paradigm of Cyber Sovereignty." *Chinese Journal of International Law* 23 (1): 25–72. https://doi.org/10.1093/chinesejil/jmae005.

Church Committee. 1975. "Covert Action in Chile, 1963-1973." Washington, D.C. https://www.intelligence.senate.gov/sites/default/files/94chile.pdf?utm_source=chatgpt.com.

CIA. 1973. "Summary, '*El Mercurio*.'" https://nsarchive.gwu.edu/document/22831-08-cia-summary-el-mercurio-february-28-1973.

CIA. 2000. "Report to Congress on CIA Activities in Chile." https://irp.fas.org/cia/product/chile/index.html.

Daghrir, Wassim. 2017. "American Foreign Policy Fiascos." *Advances in Social Sciences Research Journal* 4 (8). https://doi.org/10.14738/assrj.48.2869.

Deibert, Ron. 2015. “Authoritarianism Goes Global: Cyberspace Under Siege.” *Journal of Democracy* 26 (3): 64–78. https://doi.org/10.1353/jod.2015.0051.

Galeotti, Mark. 2019. *We Need to Talk About Putin: How the West Gets Him Wrong*. London: Ballantine Books.

George, Alexander L., and Andrew Bennett. 2005. *Case Studies and Theory Development in the Social Sciences*. BCSIA Studies in International Security. Cambridge, Mass: MIT Press.

Gross, Leo. 1948. “The Peace of Westphalia, 1648–1948.” *American Journal of International Law* 42 (1): 20–41. https://doi.org/10.2307/2193560.

Gustafson, Kristian. 2007. *Hostile Intent : U.S. Covert Operations in Chile, 1964-1974*. Vol. 1st ed. Washington, D.C.: University of Nebraska Press.

Harding, Luke. 2018. “Russian-US Tycoon Boasted of ‘Active’ Involvement in Trump Election Campaign.” *The Guardian*, September 28, 2018, sec. US news. https://www.theguardian.com/us-news/2018/sep/28/russian-us-tycoon-boasted-of-active-involvement-in-trump-election-campaign-simon-kukes. Accessed January 30, 2025.

Harmer, Tanya. 2019. “The ‘Cuban Question’ and the Cold War in Latin America, 1959–1964.” *Journal of Cold War Studies* 21 (3): 114–51. https://doi.org/10.1162/jcws_a_00896.

Hobbes, Thomas. 1651. *Leviathan, or the Matter, Forme, & Power of a Common-Wealth Ecclesiasticall and Civill*. London: Andrew Crooke. https://historyofeconomicthought.mcmaster.ca/hobbes/Leviathan.pdf.

Jamieson, Kathleen Hall. 2020. *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don’t, Can’t, and Do Know*. Oxford, UNITED STATES: Oxford University Press, Incorporated.

Jones, Seth G. 2019. “Russian Meddling in the United States: The Historical Context of the Mueller Report,” March. https://www.csis.org/analysis/russian-meddling-united-states-historical-context-mueller-report.

Kellner, Douglas. 2018. “Donald Trump, Globalization, and the Russia Connection in Election 2016.” *Cultural Politics* 14 (2): 139–52. https://doi.org/10.1215/17432197-6609032.

Kim, Jaechun. 2005. “Democratic Peace and Covert War: A Case Study of the U.S. Covert War in Chile.” *Journal of International and Area Studies* 12 (1): 25–47. https://www.jstor.org/stable/43107109.

Korab-Karpowicz, W. Julian. 2010. “Political Realism in International Relations.” Edited by Edward N. Zalta. The Metaphysics Research Lab. https://plato.stanford.edu/archives/sum2017/entries/realism-intl-relations/.

Kornbluh, Peter. 2013. *The Pinochet File: A Declassified Dossier on Atrocity and Accountability*. Rev. and Updated ed., 40th anniversary edition. New York: The New Press.

Krasner, Stephen D. 1995. “Compromising Westphalia.” *International Security* 20 (3): 115–51. https://doi.org/10.2307/2539141.

Krasner, Stephen D. 1999. *Sovereignty: Organized Hypocrisy*. Princeton: Princeton University Press. https://doi.org/10.1515/9781400823260.

Krever, Mick, and Anna Chernova. 2023. “Wagner Chief Admits to Founding Russian Troll Farm Sanctioned for Meddling in US Elections.” CNN. February 14, 2023.

https://www.cnn.com/2023/02/14/europe/russia-yevgeny-prigozhin-internet-research-agency-intl/index.html. Accessed November 30, 2024.

Landis, Fred Simon. 1975. "Psychological Warfare and Media Operations in Chile, 1970-1973." Ph.D., United States -- Illinois: University of Illinois at Urbana-Champaign. https://www.proquest.com/docview/302715768/abstract/BAB0DA8C56084F6EPQ/1.

Liaropoulos, A. 2013. "Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction?" *Journal of Information Warfare* 12 (2): 19–26. https://www.jstor.org/stable/26486852.

Margulies, Peter. 2013. "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility." *Melbourne Journal of International Law* 14 (2): 496–519. https://heinonline.org/HOL/P?h=hein.journals/meljil14&i=506.

Maschmeyer, Lennart. 2024. *Subversion: From Covert Operations to Cyber Conflict*. 1st ed. Oxford University Press. https://doi.org/10.1093/oso/9780197745854.001.0001.

McCombie, Stephen, Allon J. Uhlmann, and Sarah Morrison. 2020. "The US 2016 Presidential Election & Russia's Troll Farms." *Intelligence and National Security* 35 (1): 95–114. https://doi.org/10.1080/02684527.2019.1673940.

Mearsheimer, John J. 2001. *The Tragedy of Great Power Politics*. 1. ed. The Norton Series in World Politics. New York, NY: Norton.

Monaghan, Andrew. 2016. *The New Politics of Russia: Interpreting Change*. Manchester, England: Manchester University Press.

Morley, Morris, and Steven Smith. 1977. "Imperial 'Reach': U.S. Policy and the CIA in Chile." *Journal of Political & Military Sociology* 5 (2): 203–16. https://www.jstor.org/stable/45293026.

Mueller, Milton L. 2020. "Against Sovereignty in Cyberspace." *International Studies Review* 22 (4): 779–801. https://doi.org/10.1093/isr/viz044.

Mueller, Robert S., III. (DOJ) 2019. "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." Washington, D.C.: Department of Justice. https://www.justice.gov/archives/sco/file/1373816/dl.

Nakashima, Ellen, and Joby Warrick. 2012. "Stuxnet Was Work of U.S. and Israeli Experts, Officials Say." *Washington Post*, June 2, 2012. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html. Accessed December 4, 2024.

National Security Council (NSC). 1971. "Memorandum to Kissinger, '40 Committee Meeting, September 9, 1971-Chile'" https://nsarchive.gwu.edu/document/22827-04-national-security-council-memorandum.

National Security Council (NSC). 1972. "Memorandum for Henry Kissinger, '40 Committee Meeting-Chile.'" https://nsarchive.gwu.edu/document/22830-07-nsc-memorandum-henry-kissinger-40.

Paterson, Thomas, and Lauren Hanley. 2020. "Political Warfare in the Digital Age: Cyber Subversion, Information Operations and 'Deep Fakes.'" *Australian Journal of International Affairs* 74 (4): 439–54. https://doi.org/10.1080/10357718.2020.1734772.

Perla, Héctor. 2008. “Grassroots Mobilization against US Military Intervention in El Salvador.” *Socialism and Democracy* 22 (3): 143–59. https://doi.org/10.1080/08854300802361646.

Perloff-Giles, Alexandra. 2018. “Transnational Cyber Offenses: Overcoming Jurisdictional Challenges.” *Yale Journal of International Law*, January. https://openyls.law.yale.edu/handle/20.500.13051/6724.

Philpott, Daniel. 2010. *Revolutions in Sovereignty: How Ideas Shaped Modern International Relations*. Princeton University Press. https://doi.org/10.1515/9781400824236.

Power, Margaret. 2008. “The Engendering of Anticommunism and Fear in Chile’s 1964 Presidential Election*.” *Diplomatic History* 32 (5): 931–53. https://doi.org/10.1111/j.1467-7709.2008.00735.x.

Rashbaum, William K., Ben Protess, and Mike McIntire. 2018. “At Trump Tower, Michael Cohen and Oligarch Discussed Russian Relations.” *The New York Times*, May 25, 2018, sec. U.S. https://www.nytimes.com/2018/05/25/us/politics/michael-cohen-viktor-vekselberg-trump-tower.html. Accessed January 30, 2025.

Rudgers, David F. 2000. “The Origins of Covert Action.” *Journal of Contemporary History* 35 (2): 249–62. https://doi.org/10.1177/002200940003500206.

Sassen, Saskia. 1996. *Losing Control? Sovereignty in an Age of Globalization*. New York: Columbia University Press.

Schmitt, Michael N., and Liis Vihul. 2017. “Sovereignty in Cyberspace: Lex Lata Vel Non?” *AJIL Unbound* 111:213–18. https://doi.org/10.1017/aju.2017.55.

Schmitt, Michael N., ed. 2017. “Sovereignty.” In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., 11–29. Cambridge University Press. https://doi.org/10.1017/9781316822524.007.

Scott, Jasper. 2020. *Russian Cyber Operations: Coding the Boundaries of Conflict*. Washington, DC: Georgetown University Press.

Select Committee on Intelligence. 2017. “Open Hearing: Social Media Influence in the 2016 U.S. Election.” Washington, D.C. https://www.govinfo.gov/content/pkg/CHRG-115shrg27398/pdf/CHRG-115shrg27398.pdf.

Simović, Miodrag N., Živorad Rašević, and Vladimir M. Simović. 2020. “Cyber Warfare and International Cyber Law: Whither?” *Journal of Criminology and Criminal Law* 58 (3): 23–37. https://doi.org/10.47152/rkkp.58.3.2.

Stone, Peter, and Greg Gordon. 2018. “FBI Investigating Whether Russian Money Went to NRA to Help Trump.” McClatchy Washington Bureau. May 16, 2018. https://www.mcclatchydc.com/news/nation-world/national/article195231139.html. Accessed January 30, 2025.

Traynor, Ian. 2007. “Russia Accused of Unleashing Cyberwar to Disable Estonia.” *The Guardian*, May 17, 2007, sec. World news. https://www.theguardian.com/world/2007/may/17/topstories3.russia. Accessed December 4, 2024.

U.S. Office of the Director of National Intelligence (ODNI). 2017. “Assessing Russian Activities and Intentions in Recent US Elections.” Office of the Director of National Intelligence. https://purl.fdlp.gov/GPO/gpo76345.

U.S. Senate Select Committee on Intelligence (SSCI). 2019. “Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume I: Russian Efforts Against Election Infrastructure.” https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

Van Atta, Don. 2018. “Why They Did It: The Context of Russian Interference in the 2016 US Presidential Election.” *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4117812.

Vićić, Jelena, and Erik Gartzke. 2024. “Cyber-Enabled Influence Operations as a ‘Center of Gravity’ in Cyberconflict: The Example of Russian Foreign Interference in the 2016 US Federal Election.” *Journal of Peace Research* 61 (1): 10–27. https://doi.org/10.1177/00223433231225814.

Wills, Matthew. 2018. “The Unlikely Spy Alliance Behind the 1916 Black Tom Explosion.” JSTOR Daily. January 30, 2018. https://daily.jstor.org/the-unlikely-spy-alliance-behind-the-1916-black-tom-explosion/. Accessed January 30, 2025.

Wise, David. 1975. “The Secret Committee Called ‘40.’” *The New York Times*, January 19, 1975, sec. Archives. https://www.nytimes.com/1975/01/19/archives/the-secret-committee-called-40-at-least-in-theory-it-controls-the.html. Accessed January 28, 2025.

Zilincik, Samuel, and Isabelle Duyvesteyn. 2023. “Strategic Studies and Cyber Warfare.” *Journal of Strategic Studies* 46 (4): 836–57. https://doi.org/10.1080/01402390.2023.2174106.