Revisioning the Sources of Power in the 21st Century: Cyber Intelligence. Case Study: Russian Federation

Supervisor: Professor George-Cristian Maior, Ph.D. (Ambassador)

Doctoral Candidate: Dragoș Vetrescu

Introduction and Research Objective

This doctoral thesis, titled *"Revisioning the Sources of Power in the 21st Century: Cyber Intelligence. Case Study: Russian Federation,"* examines how intelligence operations in cyberspace (cyber intelligence) act as a force multiplier in the realm of international power politics. The research addresses a timely issue in international relations: to what extent cyber capabilities, especially those related to intelligence gathering and offensive cyber operations, can enhance a state's power and influence on the global stage. The main objective of the study is to determine the extent to which cyber intelligence can amplify a state's power, analyzing this phenomenon through the case of the Russian Federation, which is particularly important in the current international context and especially for Romania. By focusing on how Russia utilizes such cyber instruments, the thesis aims to highlight the modern dynamics of state power and to fill a gap in international relations theory regarding the impact of the cyber domain on traditional power structures.

Theoretical Framework

The study is grounded in international relations and security studies theories, especially the concepts of power politics (Realpolitik) and hybrid warfare, which it complements in an interdisciplinary manner with concepts from the field of intelligence studies. The thesis conceptualizes cyber intelligence as an emerging element of state power, capable of enhancing traditional diplomatic, military, and informational instruments. The notion of a "force multiplier" is used in a strategic sense, referring to a factor that significantly increases the effectiveness of a state's existing capabilities. In this context, the work starts from the idea that intelligence operations in cyberspace — including cyber espionage, information warfare, and other disruptive or destructive cyber actions — can multiply the effect of a state's actions without requiring recourse to large-scale conventional military force. This theoretical foundation underscores the importance of addressing cyber operations not just as technical problems, but as strategic tools in the competition for power among states.

Research Methodology

The thesis employs a qualitative methodology, specifically a comparative case study approach, following Stephen Van Evera's guidelines for structured hypothesis analysis. Through a focused and structured comparison, multiple instances (case studies) of cyber operations conducted by Russia are systematically examined. This method involves analyzing each selected case based on the same set of questions and criteria, allowing for a coherent comparison across different events. In each case, factors such as the geopolitical context, the objectives of the cyber operation, the tactics and techniques used, as well as the results or impact on the dynamics of power at the international level are taken into account. Following Van Evera's approach, the research tests the proposed hypotheses against the empirical evidence from each case, ensuring that conclusions are drawn through logical inference and process tracing (tracking causal processes). Data sources include publicly available intelligence reports (open-source), government documents, cybersecurity analyses, and academic studies, all supporting a thorough examination of how Russia's cyber intelligence activities were implemented and with what effect.

Research Hypotheses

The general objective of the research is to examine how cyber intelligence capabilities influence the dynamics of power in the international system, using Russia as a case study. Thus, the central research question is: *What is the role of cyber intelligence in the international competition for power in the cyber domain?*

From this central question derive the following secondary questions that the thesis aims to answer:

- What is cyber intelligence, and how does it function as an instrument of state power?
- How do states use cyber intelligence to amplify their geopolitical influence and counter more powerful adversaries?
- In what ways does the Russian Federation employ cyber intelligence operations to advance its strategic objectives, and what is the impact on global power dynamics?
- How might emerging technologies (such as artificial intelligence and quantum computing) shape the future of cyber intelligence in the global competition for power?

To address these questions, the analysis is guided by several fundamental hypotheses formulated on the basis of the literature and the theoretical framework:

- **States with advanced cyber intelligence capabilities can significantly amplify their power in the international system.** This hypothesis posits that states with advanced cyber capabilities (such as cyber espionage, strategic cyber attacks, and online influence operations) can achieve foreign policy objectives that exceed, in scope, what their traditional military or economic power would allow. In other words, effective cyber

operations can amplify a state's influence and effectiveness in the arena of international politics.

- **The use of cyber intelligence operations by the Russian Federation acts as a force multiplier, allowing it to challenge or disrupt a power hierarchy dominated by traditionally stronger states.** This hypothesis contends that Russia's extensive cyber espionage and intelligence-driven operations (independent variable) have measurably increased its geopolitical influence and bargaining power (dependent variable), enabling it to play a disproportionate role on the international stage. It suggests a causal link whereby Russia's cyber operations contribute to altering power dynamics in areas where, without these capabilities, Russia's influence would be more limited. This hypothesis will be tested through case studies of Russia's cyber intelligence successes (such as notable cyber attacks or strategic influence campaigns) and the consequences of these operations for Russia's position relative to its geopolitical rivals.

- **Cyber intelligence is an asymmetric tool capable of counterbalancing the conventional power asymmetry between states.** This general hypothesis suggests that even states with weaker economies or militaries can deter, coerce, or obtain concessions from stronger adversaries if they possess superior cyber intelligence capabilities. In formal terms: when a weaker state (in traditional metrics) effectively uses cyber intelligence operations (independent variable), it can partially offset or neutralize the advantages of a stronger state (dependent variable: a reduction in the influence gap or in the stronger state's ability to impose costs). This proposition is examined by studying scenarios in which cyber operations conducted by a relatively weaker actor (for example, Russian cyber actions against NATO countries) have produced effects disproportionate to that actor's overall power.

- **Integrating emerging technologies such as artificial intelligence into cyber intelligence capabilities will further amplify their impact on the international distribution of power.** This forward-looking hypothesis proposes that as states integrate artificial intelligence and machine learning into cyber intelligence activities (independent variable), the effectiveness and strategic value of these operations will increase (dependent variable), potentially leading to new shifts in the balance of power. It anticipates that early adopters of AI in cyber intelligence could gain a significant advantage, widening the gap between states with advanced cyber capabilities and those that fall behind. Evidence for this hypothesis is exploratory, based on current trends in AI applications in intelligence (such as automated threat analysis or enhanced cyber-attack strategies), and is analyzed in Chapter 6 to project these technologies' implications for power competition.

These fundamental hypotheses constitute the analytical framework for assessing Russia's behavior and the effects of its cyber campaigns, with the expectation that empirical evidence will

confirm (or nuance) the idea that cyber intelligence serves as a genuine force multiplier in the contemporary world.

Case Study: Russia's Cyber Operations

Focusing on the case of Russia, the thesis provides a detailed analysis of several landmark cyber operations attributed to Russian state actors or state-affiliated entities. Each case study examines the motives, execution, and consequences of the operation, illustrating how cyber intelligence has been used as a foreign policy tool. Notable examples include:

- **Interference in the 2016 U.S. presidential election:** The thesis examines Russia's cyber meddling in the 2016 United States presidential election. This operation involved cyber espionage (intrusion into the email systems of organizations and political figures) and information warfare (dissemination of stolen information and amplification of disinformation through social networks). The case study highlights how this cyber campaign sought to undermine democratic processes and influence political outcomes in a leading global power. The findings indicate that, although it is difficult to measure the exact impact on the election result, the operation succeeded in sowing discord and raising doubts about the integrity of the American electoral system. From a strategic standpoint, this case demonstrates Russia's ability to project power and influence inside an adversary state without resorting to direct military confrontation, aligning with the concept of cyber intelligence as a force multiplier in achieving its foreign policy objectives.

- **Cyberattacks against Ukraine:** Another significant set of examples comes from the ongoing conflict between Russia and Ukraine. The thesis details operations such as the cyber attacks on Ukraine's electrical grid in December 2015 and December 2016, which caused temporary power outages for hundreds of thousands of civilians. These unprecedented attacks on critical infrastructure demonstrated how cyber means can complement conventional military aggression (in the context of the broader Russia–Ukraine conflict) by sowing chaos and highlighting the adversary's vulnerabilities. In addition, the study examines the 2017 NotPetya malware attack which, initially targeting institutions in Ukraine (for example, by compromising a widely used accounting software in that country), evolved into a global cyber incident that caused billions of dollars in damage worldwide. Although NotPetya's indiscriminate impact far exceeded its initial target, this event underscored Russia's willingness to employ extremely aggressive cyber weapons to destabilize an adversary. Through these cases, the research shows that Russia's cyber operations against Ukraine have served multiple strategic purposes: intelligence gathering, weakening the adversary's economic and governmental functions, discouraging Western support for Ukraine, and sending a message about Russia's capabilities to the entire world.

- **Other operations and hybrid tactics:** The thesis also references other operations in the cyber and information domain, such as the 2007 attacks against Estonia (one of the first instances in which a state was targeted by massive denial-of-service attacks as a reaction to a political dispute with Russia) and various disinformation campaigns in Europe. Although these examples are not analyzed as deeply as the main case studies, they provide additional context regarding the evolution of Russia's cyber strategy. Overall, a pattern emerges in which Russian intelligence agencies (such as the GRU and FSB) have developed a versatile cyber arsenal — from pure espionage (infiltrating and exfiltrating confidential data from government or foreign organizations' networks) to psychological operations (spreading propaganda or false narratives online) — which is used in a coordinated manner to advance national interests.

Key Findings

Analysis of the Russia case study provides solid evidence that cyber intelligence has functioned as a force multiplier for Moscow's power in international politics:

- **Amplified influence and asymmetric impact:** Russia's cyber operations have allowed Moscow to act beyond the weight conferred by its conventional power. For example, by interfering in the domestic politics of the United States and various European countries, Russia managed to exert influence that typically exceeds what would be possible through its conventional means (economic or diplomatic). The ability to intervene remotely in the political processes or critical infrastructure of other states offers Russia an asymmetric instrument — one that can complicate adversaries' decision-making and impose costs without a direct military confrontation.

- **Strategic integration (hybrid warfare):** The results indicate that cyber intelligence is firmly integrated into Russia's broader "hybrid warfare" strategy — a blend of military threats, covert operations, and information warfare. Cyber tactics have been used in parallel with conventional ones (as observed in Ukraine) to maximize effect. This integration acts as a force multiplier by augmenting traditional operations; for instance, paralyzing an adversary's communications or energy supply can prepare the ground for more effective terrestrial operations or, alternatively, cyber harassment and sabotage can be employed where direct military action is not feasible.

- **Limitations and countermeasures:** The research also recognizes that although cyber intelligence provides new opportunities for exerting power, it has limits. No cyber operation to date has by itself generated decisive strategic changes — for example, cyber attacks have not independently won wars, and targets have become increasingly resilient. The case of the attacks on Ukraine's power grid shows that, while disruptive, those intrusions did not dent Ukraine's resolve nor its ability to respond. Moreover, aggressive cyber operations often draw adverse international reactions, sanctions, and improvements

in cyber defenses in the targeted states. The analysis finds that the iterative nature of cyber conflicts — action and counteraction — implies that the force-multiplying effect can diminish over time as opponents adapt. Nevertheless, in the period studied, Russia obtained considerable short-term advantages by exploiting surprise and the inherent secrecy of cyber operations.

Original Contributions of the Research

This work makes several important contributions to both the specialized literature and the practical realm of international relations in the digital age:

- **Conceptual framework:** The thesis elaborates a conceptual framework for examining cyber intelligence through the lens of power politics, treating cyber capabilities as strategic variables of state power alongside traditional elements such as military force and economic leverage. In this way, the work bridges the domain of cybersecurity and international relations theory, offering a means to analyze cyber operations in terms of power projection and balance of power.

- **Empirical analysis of the Russian case:** The research provides a comprehensive analysis of Russian cyber operations in the 2010s and early 2020s, viewed through a political-strategic lens. It systematically documents how Russia planned and executed its principal cyber campaigns and correlates them with its geopolitical objectives. This empirical contribution enriches our understanding of Russia's strategic behavior and highlights the role of intelligence services and cyber units in the conduct of Russian foreign policy in the digital domain.

- **Methodological innovation:** By applying a structured comparative case study methodology (following Van Evera's model) to the field of cyber conflict, the thesis demonstrates the utility of rigorous qualitative approaches in studying cyber warfare. It shows that qualitative methods can be successfully applied in a field often dominated by technical analyses, encouraging a more theory-driven examination of cyber incidents. This validated approach is a contribution to research design in security studies, illustrating how hypothesis testing in a qualitative manner can be fruitfully employed in the context of cybersecurity.

- **Implications for policy and theory:** The thesis's findings have implications for both policymakers and the development of international relations theory. For decision-makers, understanding cyber intelligence as a force multiplier underscores the need to strengthen cyber defenses and counter-intelligence capabilities; states must recognize that even seemingly weaker adversaries can cause significant damage or wield disproportionate influence through cyber means. For international relations theory, the research suggests that existing theories of power (especially realist perspectives on the balance of power

and deterrence) should be updated to include the cyber dimension. The notion of deterrence, for instance, becomes more complex when covert cyber actions blur the line between war and peace. In this way, the thesis offers an original perspective on integrating the cyber dimension into concepts of national power and security.

Conclusions and Relevance

The case of Russia illustrates the general trend that cyber intelligence has become an indispensable component of power dynamics in the modern era. The thesis concludes that, when exploited effectively, cyber intelligence operations act as a true force multiplier: they amplify the reach and impact of a state's endeavors beyond what would be possible through conventional means. In the current international system, where major powers often avoid direct armed conflict due to high costs and risks, cyber operations occupy a strategic niche – allowing states like Russia to pursue aggressive objectives under the cover of plausible deniability and below the threshold of formally declaring war.

The research underscores that global power dynamics are evolving. Mastery in a domain such as cyberspace can translate into diplomatic advantages, coercive capabilities, and influence in a manner that challenges conventional power hierarchies. Therefore, understanding and integrating the cyber dimension in both the practice of foreign policy and in international relations theory becomes essential. The lessons drawn from Russia's experience serve as a reference point for other state actors and for researchers seeking to understand how power is exercised in the digital era, reinforcing the thesis's central argument regarding the transformative role of cyber intelligence in world politics.