ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Assessing Power and Hierarchy in Cyberspace: An Approach of Power Transition Theory

Enescan Lorci | College of Social Science, Institute of China and Asia-Pacific Studies, Taiwan | ORCID: 0000-0003-0111-6331

Abstract

This study explores the application of Power Transition Theory (PTT) to cyberspace, aiming to establish a comprehensive framework for understanding and measuring cyber power. Utilizing PTT's national power model, the research treats states as rational and unitary actors, integrating the rational actor model to assess state behavior in cyberspace. The objectives include defining cyber power, developing a novel metric for its evaluation, and categorizing states within a hierarchical structure of cyber power. By analyzing key components such as data resources, digital economic strength, and cyber political capacity, the study provides a nuanced understanding of cyber power dynamics. The results demonstrate that the traditional IR theories retain relevance in the cyber domain, offering a valuable lens for comprehending global cyber governance and geopolitical competition. This foundational work sets the stage for future analyses of power transitions within cyberspace, highlighting the critical interplay between traditional power metrics and emerging digital landscapes.

Keywords

power transition theory, cyber power, power assessment, internet population, digital economy, cyber political capacity

Received: 25.03.2024

Accepted: 20.06.2024

Published: 27.07.2024

Cite this article as:
E. Lorci "Assessing Power and Hierarchy in Cyberspace: An Approach of Power Transition Theory," ACIG, vol. 3, no. 2, 2024, DOI: 10.60097/ACIG/190481

Corresponding author:
Enescan Lorci, College of Social Science, Institute of China and Asia-Pacific Studies, Taiwan; E-mail: enescanlorci@g-mail.nsysu.edu.tw
0000-0003-0111-6331

1. Introduction

Following the inception of the internet, American policymakers recognized its potential significance not only in matters of security but also in terms of its economic and ideological impact [1, p. 78]. This critical role of the internet became particularly evident during the Clinton presidency, prompting the American government to take measures aimed at regulating the advancement and dissemination of internet-related technologies. In response to the increasing involvement of governments in cyberspace during this period, John Perry Barlow, a cyberlibertarian activist, composed his renowned "Declaration of Independence of Cyberspace" in 1996 [2]. In this declaration, Barlow contended that cyberspace should remain free from the interference of governmental entities, asserting that it is not a domain amenable to the practice of sovereignty by governments from the industrialized world.

Barlow's perspective emphasized that governments should not exercise hegemonic control over cyberspace. Despite the establishment of the Internet Corporation for Assigned Names and Numbers (ICANN) in 1998, which granted the American government a significant degree of influence over cyberspace, the ideals of a free and open cyberspace, as well as the unimpeded flow of information, were conducive to furthering American objectives of disseminating liberal economic principles and democratic values worldwide in the post-Cold War era [3].

In this context, the United States has significantly influenced the progression of the internet and other Information and Communication Technologies (ICTs) within the global landscape, including cyberspace. Consequently, the governance of this emerging domain has been executed through a model that aligns with American objectives, referred to as the "Multilateral Governance" model [4]. Under this model, decision-making authority over cyberspace is shared among governments, non-governmental organizations, private technology companies, and individual actors, all of whom influence the governance framework.

Nonetheless, over time, geopolitical dynamics have resurfaced and begun to extend their reach into the cyber realm, transforming cyberspace into a newfound arena for competition and power politics among major global powers [5]. The escalating dissatisfaction expressed by China and Russia concerning the existing structure of cyberspace, coupled with the United States' aspiration to uphold its longstanding dominance in this domain, underscores the evident role of power politics in shaping 21st-century great power

competition over cyberspace [6]. In any competition, determining each participant's position necessitates applying suitable metrics, which also holds true for the context of great power competition within the cyberspace realm. Assessing a state's relative standing vis-à-vis others requires evaluating its power capacity to compete effectively in cyberspace.

Assessing national power is a well-established endeavor, traditionally relying on metrics such as economic size, military prowess, population, and other tangible indicators. Nevertheless, the evaluation of cyber power presents a distinctive and intricate challenge [7]. Unlike conventional measures of national power, gauging cyber power is a relatively novel and arduous task [8]. Addressing this complexity necessitates an initial endeavor to precisely define power within cyberspace. Only upon establishing a clear conceptual framework for cyber power can a viable model for its measurement be formulated [9].

Following cyberspace's discernible impact on world politics, scholars of international relations have displayed varied reactions. Some scholars have avoided incorporating cyberspace into their studies, relegating it to low politics. Others have perceived cyberspace as a novel domain that defies the application of traditional international relations (IR) theories. In contrast, many international relations scholars have asserted that traditional IR theories can retain their relevance within cyberspace and have endeavored to apply them to the cyber domain.

For instance, Beltz and Steven adopted Barnett and Duvall's taxonomy for national power and adapted it to cyberspace to conceptualize cyberpower [10, p. 33]. Similarly, Joseph Nye extended his notions of hard and soft power to the context of cyber power [11]. Despite their differing approaches, these scholars shared a common belief in the potential utility of traditional IR theories within cyberspace. They contend that such theories can serve as valuable starting points in comprehending this emerging domain and the competitive dynamics that unfold within it.

In alignment with the abovementioned perspective, this research also subscribes to the notion that IR theories remain relevant and applicable in cyberspace. Embracing this belief, the study applies the Power Transition Theory (PTT) to cyberspace, aiming to achieve several objectives. Firstly, the research endeavors to define cyber power, offering a novel metric for its assessment akin to the model presented by PTT for evaluating national power. Moreover,

beyond proposing a model for measuring cyber power, the study introduces a novel categorization scheme for states in cyberspace, classifying them into four distinct categories: global cyber leaders, cyber great powers, cyber-dependent powers, and non-cyber powers. This classification serves as a valuable contribution to the field, providing a nuanced understanding of the differing positions and roles assumed by states within the cyber domain.

It is essential to clarify that the study does not address the concept of "power transition" within cyberspace at this initial stage. Instead, its primary aim is to define and propose a novel measurement method for national cyber power, thereby positioning states within a hierarchical order. By borrowing PTT's national power definition and measurement model, this research establishes the relevance of traditional IR theories to the cyber domain. This foundational work is crucial as it sets the stage for future analyses of power transitions in cyberspace, which can only be thoroughly examined once cyber power has been accurately measured using the proposed model.

Critics might argue that applying PTT to cyberspace without directly exploring "transition" dynamics is premature. However, this study is a preliminary effort to introduce an IR perspective on the definition and measurement of cyber power. It lays the groundwork for future research. The proposed model must be utilized to measure national cyber power comprehensively and subsequently explore the dynamics of power transitions within this context.

By applying traditional IR theory to cyberspace and demonstrating its applicability, this research addresses a significant gap in the existing literature. It also puts forward an innovative model for measuring cyber power and provides valuable insights into the hierarchical structure of states within cyberspace. These substantial contributions offer a new lens to understand global cyber governance and geopolitical relations in this emerging and critical domain.

The study is organized as follows to achieve these objectives. First, it reviews the literature on definitions and measurements of cyber power, situating the research within existing scholarship and highlighting its contributions. Next, it discusses the hierarchical categorization of countries in cyberspace. Subsequently, the study provides a detailed exposition of PTT's national power model, elucidating its theoretical framework and approach to defining and assessing cyber power. This structured approach contributes to the international discourse on cyber power and sheds light on the

ongoing competition for cyber dominance among major global actors. By offering a comprehensive understanding of cyber power, its dynamics, and its impacts on global affairs, this research aims to inform policymakers about the implications of their actions in cyberspace, ultimately striving to create a safer cyber environment for all stakeholders.

2. Intersection of Cyberspace, Power, and International Relations

According to Nye, the concept of power lacks a universally accepted definition and remains subject to contestation, with individual interpretations reflecting one's interests and values [11]. For instance, realist scholars in International Relations emphasize military power as a cornerstone of national power [12]. On the other hand, liberal perspectives on power encompass a broader spectrum, encompassing non-coercive means to achieve desired outcomes. In the constructivist framework, power is viewed as a socially constructed phenomenon influenced by prevailing ideas, norms, and identities. Here, power extends beyond material capabilities, encompassing the capacity to shape and influence the prevailing norms and values that inform state behavior [13].

Despite the various descriptions of power put forth by different schools of thought in the discipline, a common thread prevails: power is widely acknowledged as a crucial instrument for achieving desired outcomes in international politics [14]. The quantification of power has become a central concern for states, as it enables the assessment of the feasibility and effectiveness of particular actions. States with greater power are likelier to advance their objectives than weaker states. Consequently, power measurement has garnered significant academic attention, mirroring the importance accorded to power and facilitating comparative assessments between different actors, which has become a pivotal activity for decision-makers. When evaluating national power, numerous factors are considered, including territory, wealth, military strength, armies, navies, and military arsenals. These tangible indicators provide insight into a state's potential and capacity to exert influence in the international arena [7].

Unlike material power, the notion of power and its quantification in cyberspace has emerged as a relatively recent focus of academic inquiry. Inkster underscores the significance of assessing power by contending that the absence of reliable metrics could lead to mission failure [8]. States must gauge their power and that of their

adversaries to ensure their security. However, the intricacies of assessing power in cyberspace necessitate a preliminary explication of the concept itself. Without a comprehensive understanding of cyber power, any measurement strategy would prove ineffective [15]. Consequently, a clear and nuanced description of cyber power becomes a foundational prerequisite for developing an effective and meaningful approach to measuring it.

The involvement of IR scholarship in cyberspace dates back to the late 1990s and early 2000s, when the internet and related technologies began to play a crucial role in national security, the economy, and foreign policy objectives. Consequently, a significant body of IR literature has emerged, focusing on cyberspace, cyber power, and cyber warfare from offensive and defensive perspectives.

One of the early seminal works in this field is by Arquilla, who discussed the concept of cyber war and its potential impact on future conflicts, highlighting the strategic significance of cyberspace in international relations [16]. Martin C. Libicki analyzed how control over information can influence the battlefield, affect decision-making processes, and disrupt adversaries' operations. He emphasized the importance of protecting one's information infrastructure while targeting and exploiting vulnerabilities in opponents' systems [17].

Manuel Castells introduced the concept of the network society, where digital networks significantly shape power dynamics and international relations [18]. Similarly, Saskia Sassen explored how globalization and digital technologies influence state sovereignty and global governance, providing foundational insights into understanding cyber power [19].

Keohane and Nye examined how the information age transforms power structures and interdependence among states. Their work laid the groundwork for understanding cyber power in IR [20]. In "*Information Technologies and Global Politics: The Changing Scope of Power and Governance*," Rosenau and Singh explored how power is redefined in the context of information technologies [21]. They argued that cyber power encompasses control over IT infrastructure, cyber capabilities, and the ability to influence information flows, extending beyond traditional state-centric views and recognizing the significant roles played by non-state actors.

Nissenbaum integrated ethical considerations with IR theories to discuss the implications of cybersecurity for national and international security, highlighting the moral and strategic dimensions of cyber

power [22]. Chadwick, in *"Internet Politics: States, Citizens, and New Communication Technologies,"* explored how the internet and digital communication technologies influence political power and state-citizen interactions, which are relevant to IR and cyber power [23].

Deibert and Rohozinski analyzed how state actors exert control over cyberspace and the impact of these actions on international security dynamics. Their work integrates concepts from IR theories, such as realism and constructivism, to explain the strategic behavior of states in the digital realm [24]. Choucri, in "Cyberpolitics in International Relations," provided a comprehensive examination of how cyberspace intersects with traditional IR theories, discussing how concepts like power, sovereignty, and interdependence are redefined in the context of global cyberspace [25].

Jon R. Lindsay examined the Stuxnet cyber-attack through the lens of IR theory, mainly focusing on deterrence and coercion. He argued that traditional concepts of military power and strategy apply to understanding cyber operations and their impact on international relations [26]. Nye posited that cyber power entails the capacity to achieve desired outcomes by leveraging electronically interconnected information resources within the cyber domain. Conversely, Armistead focused on the role of information in describing cyber power, defining it as the control over a greater volume of information (data) relative to other actors [15].

Eventually, although these diverse perspectives reflected the evolving and multifaceted nature of cyber power and underscored the complexities involved in defining and understanding this concept within the context of cyberspace, it is essential to acknowledge their limitations because, in many of these approaches, the authors see developments in cyberspace either from a defensive or offensive perspective. However, this study argues that defining cyber power solely based on defensive or offensive cyber capabilities may lead to erroneous assessments, rendering assessment of cyber power inconsequential [9].

Instead, a more comprehensive approach is necessary, wherein a cyber-capable state exhibits proficiency in safeguarding the integrity of its cyberspace through vigilant monitoring, timely patching, and proficient network system definition. In addition to defensive capabilities, a cyber-capable state must demonstrate the capacity to manage, manipulate, and effectively navigate vast volumes of data crucial for modern economies and networked military operations [27]. The ability to generate intelligence and strategically wield

cyberspace to exert influence is also imperative. In sum, any definition of national cyber power ought to adopt a holistic approach, considering all facets of the cyber domain beyond mere considerations of defense or offense [27]. Embracing this comprehensive perspective will enable a more accurate and insightful assessment of cyber power, avoiding oversimplifications and yielding more meaningful results in cyber power measurement and analysis.

In this context, this study tries to adopt a holistic approach to understanding cyber power and its assessment, which aims to achieve this by focusing on the objectives pursued by a country within cyberspace. This perspective is in line with the insights provided by scholars like Armistead, who underscore the significance of considering the "context" when defining power [15]. Similarly, Nye argues that the statement of "actor A has power" lacks substantial meaning without specifying the specific scope or purpose for which that power is wielded, i.e., power "to do what [11]." Hence, in the discourse on power in cyberspace, a pertinent point of departure is to inquire into the objectives states seek to accomplish through their cyber capabilities. A comprehensive understanding of the context in which their power is exercised is established by elucidating the aims and desired outcomes that countries aspire to achieve within cyberspace.

Thus, this study argues that effectively assessing cyber power involves assessing a country's capacities to actualize the objectives it has set for itself in cyberspace. Such an evaluation yields reliable metrics for gauging a country's cyber power's extent and potential to influence and shape outcomes in this dynamic domain.

Assessing cyber power from the perspective of "objectives," the notion of standardizing the concept of cyber power may face challenges due to the potential variations in objectives in cyberspace among different countries. While it is true that objectives may vary somewhat, it is essential to recognize that many objectives are shared among rational states. Thus, analyzing this issue through the lens of the "rational state" assumption can provide valuable insights. When considering the question, "What would a rational state seek to achieve in cyberspace?" the answers likely exhibit significant commonalities. For this reason, this study adopts the assumption of a "rational state in cyberspace," which allows for generalizing objectives in cyberspace.

By applying this rational state concept to cyberspace, this study distinguishes itself from prior studies and makes valuable

contributions to ongoing discussions. This approach acknowledges the common ground among rational states regarding their objectives in cyberspace, facilitating a more comprehensive understanding of the factors driving cyber power dynamics. By incorporating the rational state assumption, the study provides a framework that accommodates shared objectives and enables a more cohesive and comparative analysis of cyber power among different states. Consequently, the research offers new perspectives and insights that contribute to advancing knowledge and dialogue on cyber power in the contemporary international arena.

Nonetheless, it is essential to acknowledge that despite sharing rational motivations, some countries might encounter challenges in promptly implementing their intentions or using their capabilities. Such obstacles can arise due to the country's regime type and bureaucratic structure, which may affect the speed and efficiency of decision-making processes. Consequently, the domestic political structure can influence a country's cyber power. Thus, it is crucial to consider domestic factors when assessing state cyber power.

In this particular context and under the rational state assumption, this research focuses on three critical objectives related to cyber power. These objectives are pivotal for a rational state striving to secure cyberspace and advance its interests in this domain. To measure a country's capabilities in achieving these objectives, the study employs a set of 30 domestic and international indicators, which serve as evaluative criteria. (see Table 1).

Before introducing these capabilities, it is important to emphasize that the model presented in this research is rooted in the PTT's state power assessment strategies. Therefore, it is essential to provide a concise overview of the PTT's key principles and concepts, especially in regard to power. Subsequently, the study will proceed to apply the PTT's power assessment framework within the context of cyberspace, first by introducing hierarchical situations in international cyberspace and then introducing a model for assessing a state's cyber power.

3. PTT's Approach to National Power and International Hierarchy

The Power Transition Theory (PTT) 's central premise revolves around significant power shifts within the international system, leading to periods of either stability or conflict. These shifts are often characterized by the ascent of a challenger power

Table 1. Synthesized model for cyber power assessment.

Three vital objectives of the rational state in cyberspace	Indicators for the assessment of capabilities	
	Domestically	**Internationally**
Attainment of a substantial internet population and ownership of data	Effectiveness of domestic cyber intelligence	Effectiveness of international cyber intelligence
	Effectiveness of domestic cyber surveillance	Effectiveness of international cyber surveillance
	Effectiveness of domestic offensive cyber operations	Effectiveness of international offensive cyber operations
	Effectiveness of domestic defensive cyber operations	Effectiveness of international defensive cyber operations
	Effectiveness of domestic cyber influence operations	Effectiveness of international cyber influence operations
Cultivation of a robust digital economy	Amount of domestic broadband infrastructure (ICTs, Internet, and IT(data) Sectors), ICT employment	Amount of international broadband infrastructure (ICTs, internet infrastructure, 5G, AI,IT)
	Level of domestic e-commerce sales	Level of international e-commerce sales
	Domestic digital payment adoption	International digital payment adoption
	Share of ICTs in total GDP And ICT access and use by households and individuals,	Share of ICT exports in the country's overall export
	Effectiveness of digital government services	Digital economic trade agreements
Cultivation of a high degree of cyber political capacity	Effectiveness of capacity building and awareness	Capability of determining international cyber norms, principles, standards, and developments (International cyber governance)
	Capability of making effective National cybersecurity strategies	International treaties and agreements
	Capability of making and implementing Cybersecurity Laws and Regulations	Participation in International Fora
	Capability of data gathering protection and privacy	Participation in Cybersecurity Cooperation Agreements
	Quick and effective incident response and coordination	Active cyber public diplomacy

that challenges the existing dominant power. PTT posits that such power transitions bear substantial consequences for international politics, influencing the potential for conflict or cooperation among states. As power constitutes a major determinant of war and peace in the international system, PTT places great emphasis on explaining its dynamics [28].

PTT conceptualizes national power as a composite of three crucial elements: population, economic productivity, and political capacity [29]. The first element is population, which encompasses the sheer number of people and the quality of human resources. This includes the population's skills, education, health, and demographic characteristics. A robust and skilled population is essential for sustaining economic growth, supporting national defense efforts, and contributing to innovation and technological advancements. A large population provides a substantial labor force necessary for industrial and economic development. It also offers a wide recruitment base for the military, enhancing a nation's defense capabilities. Furthermore, the population's age structure plays a critical role; a younger, dynamic workforce can drive economic productivity, whereas an aging population might strain social services and economic growth [30].

The second element is economic productivity, typically measured by a country's Gross Domestic Product (GDP). Economic productivity reflects a nation's capacity to generate wealth and economic output, which underpins its ability to invest in various sectors critical for national power, such as military capabilities, technological advancements, and infrastructure development [31]. A strong economy enables a country to sustain prolonged periods of conflict by financing military operations, maintaining sophisticated defense systems, and ensuring economic resilience in the face of blockades or sanctions. Economic productivity also enhances a nation's diplomatic leverage as economic aid and trade agreements become tools of influence. Moreover, a thriving economy attracts global investments and fosters innovation, further solidifying a nation's competitive edge in the international arena.

The third element is political capacity, referring to the effectiveness of a country's political system in mobilizing resources from its citizens and deploying them efficiently to achieve national objectives. Political capacity involves the ability of the state to enact policies, maintain internal stability, and project power externally [32]. An efficient political system can harness the potential of a large population and a productive economy by ensuring that resources are directed toward strategic goals. This includes the capability to implement sound economic policies, maintain law and order, provide public goods, and manage crises. Political stability and governance quality are crucial for fostering an environment where economic and human resources can thrive. Political capacity also encompasses the ability to form strategic alliances and exert influence in international institutions. A politically capable state can navigate complex

global challenges, mediate conflicts, and shape international norms and rules to its advantage.

These three components, population, economic productivity, and political capacity are interdependent and mutually reinforcing. A nation may have a large, economically productive population, but its power potential remains constrained without an adept political system to harness and utilize these resources effectively. Conversely, a small nation with a highly efficient political system can maximize its limited resources to achieve significant influence.

For instance, China's rise is often attributed to its large and increasingly skilled population, rapid economic growth, and a political system capable of mobilizing resources for large-scale projects and strategic initiatives. On the other hand, countries with abundant resources but weak political systems, such as some oil-rich states, may struggle to convert their potential into sustained national power. Thus, PTT views power as a product of a country's harmonious domestic components. This holistic approach underscores that national power is not merely a function of economic or military might but also depends on the quality and effectiveness of political institutions and the nation's human capital. Understanding these dynamics is crucial for analyzing power transitions, as shifts in the relative power of states can lead to significant changes in the international order. By examining how national power is constructed and distributed within this framework, PTT provides valuable insights into the stability and transformation of the global system.

On the other hand, in the context of PTT, the distribution of power within the international system is depicted as a hierarchical structure. At the apex of this hierarchy lies the dominant power, which exercises control over a significant portion of the system's resources and sets the rules and norms that govern international interactions. The dominant power acts as the primary architect of the international order, establishing institutions and frameworks that reflect its interests and values [33, p. 86].

Below the dominant power are the great powers, which possess considerable capabilities and resources, though not to the extent of the dominant state. Great powers play significant roles in shaping international politics and can challenge or support the dominant power's leadership. They have substantial military, economic, and political influence, allowing them to impact global governance and security dynamics.

Further down the hierarchy are the middle powers with moderate resources and capabilities. Middle powers often act as stabilizers within the international system, supporting the existing order or advocating for incremental changes. They may form coalitions with other states to amplify their influence and contribute to regional stability and development.

At the bottom of the hierarchy are the minor powers, which possess the fewest resources and capabilities within the system. Small powers are often more vulnerable to external pressures and have limited ability to influence global politics independently. They typically align with more powerful states or international organizations to safeguard their interests and security.

This hierarchical arrangement underscores the varying degrees of influence and authority among states in the international system. The dominant power, with its superior resources, assumes the role of founder, rule-maker, and value determinant of the international system [34]. Meanwhile, great, middle, and minor powers navigate the international landscape based on their respective capabilities and positions within the hierarchy. This structure shapes the interactions between states, influencing the patterns of conflict, cooperation, and competition in global politics. According to Rachel, understanding these dynamics is crucial for analyzing power transitions, as shifts in the relative power of states can lead to significant changes in the international order. By examining how national power is constructed and distributed within this hierarchical framework, PTT provides valuable insights into the stability and transformation of the global system. Following this elucidation of PTT, the subsequent section of this research will establish an international power hierarchy in cyberspace and develop a novel approach to understanding and evaluating cyber power inspired by the foundational principles of PTT (see Figure 1).

4. Hierarchy in Cyberspace

Hierarchy in cyberspace posits that a dominant cyber power occupies the pinnacle, exerting control over most resources in the cyberspace domain. This dominance is characterized by a substantial command over critical infrastructures, advanced technological capabilities, and significant cyber intelligence assets. Importantly, as in Power Transition Theory (PTT), being the dominant cyber power does not necessarily equate to being a hegemon [29]. While a hegemon exercises unrivaled supremacy and exerts influence unilaterally, the dominant cyber power's influence is more nuanced and collaborative.

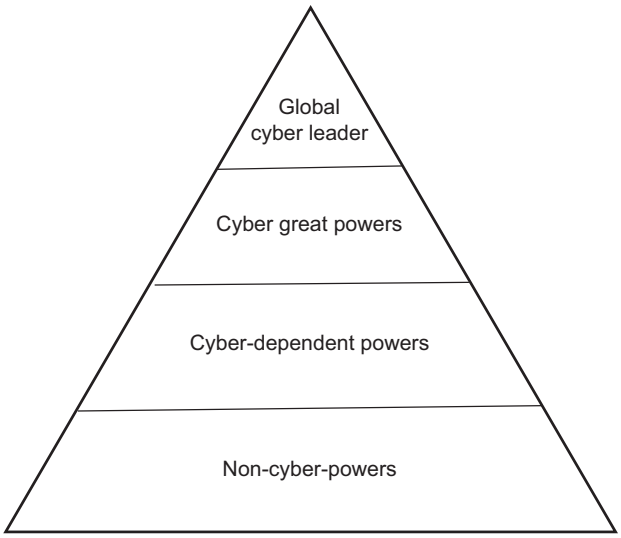

Figure 1. Cyberspace power hierarchy.

Instead, the dominant cyber power assumes a leadership role in advancing technical developments within cyberspace and in shaping the standards, norms, principles, and regulations governing cyberspace. This involves pioneering innovations in cybersecurity, artificial intelligence, and data governance that set benchmarks for others to follow. By establishing frameworks and protocols for secure and efficient cyber operations, the dominant cyber power influences global practices and policies.

Furthermore, the dominant cyber power aligns these standards and norms with its national and allies' interests. This alignment is achieved through diplomatic efforts, international agreements, and active participation in global forums dedicated to Internet governance and cyber norms. By doing so, the dominant cyber power ensures that the regulatory environment of cyberspace reflects its strategic priorities, such as the promotion of a free and open Internet, protection of intellectual property rights, and establishment of robust cybersecurity measures.

In addition to technical and regulatory leadership, the dominant cyber power also plays a crucial role in shaping the geopolitical landscape of cyberspace. This includes leveraging its cyber capabilities to influence global economic activities, conduct cyber espionage, and engage in strategic cyber operations that reinforce its geopolitical objectives. Through such activities, the dominant cyber power can project its influence across borders, affecting the

internal dynamics of other states and steering international relations in favorable directions.

Following the dominant cyber power, the cyber power hierarchy includes several cyber great powers, each wielding substantial influence within cyberspace. The stability and maintenance of the cyberspace system largely depend on the satisfaction of these cyber great powers with the existing framework [35]. Domestically, cyber great powers demonstrate capabilities in data control, possess robust digital economies, and exhibit strong political cyber capacity. However, their willingness to exercise their cyber-political capacity internationally is contingent upon their satisfaction with the prevailing system.

For example, the European Union (EU), a great cyber power with significant capabilities, refrains from challenging the USA to assert its cyber-political capacity internationally. This is primarily due to the existing structure of international cyberspace, which aligns with the EU's national interests by emphasizing freedom, free flow of information, liberal economic principles, and decentralized decision-making processes. In contrast, despite possessing substantial cyber capabilities, including vast data control, robust digital economies, and effective domestic cyber political capacity, other great cyber powers such as China and Russia remain motivated to enhance their cyber political capacity on the international stage [36]. This is driven by their dissatisfaction with the current system, particularly the governance model of cyberspace. Unlike the USA and its Western allies, China and Russia advocate for a more pronounced role of the state in cyberspace and full sovereignty of states in this domain [37]. Consequently, these challengers, having already bolstered their other cyber capabilities, are now earnestly endeavoring to augment their international cyber-political capacity to reshape the USA-led structure of cyberspace.

After the cyber great powers, many cyber-dependent powers are situated within the cyber power hierarchy. These states possess certain cyber capabilities, including a substantial internet population and a degree of digitalization with accessible internet services for their citizens. However, they rely on foreign technologies for critical services such as internet infrastructure, telecommunication technologies, 5G, and AI. Consequently, while cyber-dependent countries have control over some data due to their internet population and digital aspects of their economy, their reliance on external actors to develop these capabilities renders them vulnerable in terms of cyber security. This vulnerability is particularly evident in examples of cyber-dependent powers in many developing nations.

Finally, at the bottom of the international cyberspace hierarchy, we find numerous non-cyber powers characterized by the absence of a fundamental component and source of cyber power, namely the internet population. These states exhibit an internet penetration rate of less than fifty percent and face the challenge of expensive internet services beyond the affordability of their citizens. The World Wide Web Foundation, Alliance for Affordable Internet employs a metric indicating that for internet services to be deemed affordable, 1GB of data should cost 2% or less of the average monthly income [38]. However, numerous African countries fail to meet this criterion, as exemplified by Equatorial Guinea, where 1GB of mobile data costs a significant $49.67 [38]. Sao Tome Principe and Malawi follow closely with costs of $30.97 and $25.46 per gigabyte, respectively. In addition, Chad and Namibia are in the top five, with average prices of $23.33 and $22.37 per gigabyte, respectively. These circumstances underscore the challenges faced by non-cyber powers in attaining affordable and accessible internet services, limiting their capacity to partake in the realms of cyberspace and cyber power.

This hierarchical model of cyber power provides a nuanced understanding of states' various roles and capacities within the international cyberspace arena, reflecting the complexity and multifaceted nature of power dynamics in the digital age. By categorizing states into different tiers based on their cyber capabilities, this model elucidates the diverse ways in which states engage with and exert influence in cyberspace

5. Translating PTT's National Power Model to Cyberspace

During the 1950s, the PTT emerged as a distinct theoretical framework, offering a critical perspective on the prevailing balance of power theory. PTT's foundational arguments rest upon key assumptions, notably asserting that states represent the primary units of analysis in the international system and that they act as rational entities in their interactions [39]. The primacy of states as central actors in the international realm found significant acceptance among various international relations theories in the physical domain. However, the applicability of such assumptions encountered challenges when applied to the context of cyberspace.

The distinctive nature of cyberspace complicates the traditional state-centric perspective endorsed by the PTT. Notably, the diffusion of power in the cyber domain transcends the conventional state-centric paradigm, as multiple actors assume prominent

roles alongside states. This includes private companies, endowed with substantial capabilities in the cyber realm, and individual actors who significantly influence and shape cyberspace dynamics [39].

Nye's analysis in cyberspace discerns three distinct actor categories: governments, organizations with well-structured networks, and individuals. According to Nye it is true that the power diffused among these actors however the distribution of power does not imply a state of equality in capabilities [11]. Governments, due to their possession of substantial resources, wield greater capabilities within the cyber domain. Moreover, the geographical underpinnings of the internet's physical infrastructure, coupled with governments' sovereign authority over territorial spaces, endow location with continued significance as a valuable resource in cyberspace [40]. In addition, geography serves as a basis for governments to exercise legal coercion and control, as a government can exert power extraterritorially if a market is sufficiently extensive [41]. Non-state actors in the cyber realm must safeguard their legal standing and brand reputation, necessitating strong incentives for compliance with local legal structures. This adherence to the established legal framework becomes another resource of power for governments, given their authority in shaping domestic legal systems [4].

Consequently, despite power diffusion in cyberspace, this does not translate to power equalization, as states remain the primary actors with superior resources and capabilities [11]. Thus, this research assumes state as unitary actor in cyberspace and predominantly focuses on states and their cyber objectives, aiming to discern hierarchy in cyberspace and cyber power dynamics.

As expounded previously, the present research endeavors to conceptualize cyber power through the lens of a rational state's objectives in cyberspace. Building upon the PTT's elucidation of population, economic productivity, and political capacity as pivotal constituents of national power, this study posits three primary objectives that a rational state seeks to pursue in the cyber domain. First, attaining a substantial internet population and data ownership means a rational state aims to foster a sizeable and active internet user base within its territorial confines, signifying the penetration and accessibility of cyberspace to its population. Moreover, the possession and control of data resources become a critical objective, as data ownership is a valuable asset, contributing to insights, analytics, and potential competitive advantages [42].

Second, cultivating a robust digital economy is based on the idea that the rational state endeavors to nurture and bolster its digital economy, recognizing the profound economic implications of the cyber realm. A thriving digital economy is indicative of a vibrant ecosystem encompassing electronic commerce, online transactions, digital services, and innovative technology sectors, enhancing economic growth and competitiveness on the global stage [43].

Finally, cultivating a high degree of cyber political capacity argues that a rational state seeks to amass a considerable level of cyber political capacity, denoting its ability to wield influence, enact policies, and control cyber activities domestically and internationally. This capacity encompasses regulatory frameworks, legislative measures, and governance mechanisms aimed at safeguarding cyber interests, ensuring cyber stability, and projecting cyber influence on the global political landscape [44].

This research undertakes an evaluative examination of the objectives stated earlier to comprehensively understand the cyber power of a rational state within cyberspace. For each objective, the research assesses specific indicators of capabilities to measure state cyber power, differentiating between a country's domestic and international capabilities. The rationale behind analyzing indicators separately for domestic and international contexts derives from the theoretical alignment with the PTT in its approach to national power.

Analogous to PTT's premise that a nation's power hinges on its domestic dynamics, this research contends that a country's cyber power is similarly contingent upon its domestic cyber capabilities. Indeed, a country is unlikely to emerge as a significant international cyber power without first establishing a certain degree of domestic cyber power [45]. For instance, exerting considerable control over the international flow of data is improbable without prior adeptness in managing domestic data flows and enhancing corresponding capabilities. Hence, an accurate assessment of the country's cyber power necessitates an analysis of both domestic and international capabilities for each objective.

Next, the research analyzes each objective individually, expounding upon their significance in determining the cyber power of a rational state in cyberspace. By delving into the multifaceted dimensions of each objective, the research endeavors to offer a nuanced comprehension of the interplay between a state's strategic cyber pursuits and its overall cyber power within the dynamic and evolving cyber landscape.

5.1. Attainment of a Substantial Internet Population and Ownership of Data

Government ownership of data holds considerable significance in cyber power and governance. First and foremost, it empowers governments with access to vast information repositories, which can be leveraged for various purposes, including intelligence gathering, law enforcement, and national security initiatives. By exercising data ownership, governments can employ sophisticated data analytics, machine learning, and artificial intelligence techniques to derive valuable insights from the collected information, contributing to informed decision-making and policy formulation [46].

Furthermore, data ownership facilitates the capacity of governments to monitor, supervise, and safeguard their internet populations against cyber threats and malicious activities [47]. Comprehensive datasets enable governments to conduct cyber surveillance, detect potential threats, and respond to cyber incidents promptly and effectively. Moreover, data ownership is closely linked to the protection of critical infrastructure, as governments can employ data-driven risk assessments to bolster the resilience of essential digital systems and networks [47].

As previously expounded in this study, the significance of domestic cyber capabilities is pivotal in positioning a state as a significant actor in the international cyberspace arena. Within this context, internet population and data ownership are crucial in shaping a nation's overall cyber power. These two concepts are intricately linked, as the size and engagement of the internet population directly influence the generation and accumulation of substantial data arising from their online interactions, activities, and behaviors. Drawing upon the PTT's emphasis on population as a fundamental element of national cyber power and recognizing its role as a resource for economic productivity, this research similarly underscores the internet population's value as a reservoir of data.

As the number of individuals accessing the internet and actively participating in online services continues to rise, the volume and diversity of data generated through their digital activities undergo an exponential expansion. This data encompasses a broad spectrum of information, ranging from personal details to digital communications and user behavior patterns [48]. The data, in turn, assumes a critical asset for states seeking to strengthen their cyber power. Through effective data ownership and governance, governments can harness this vast repository of information to gain insights, make informed decisions, and enhance their cyber capabilities.

Comprehensive data ownership derived from the internet population empowers governments with numerous advantages. It facilitates the development and deployment of advanced data analytics, machine learning, and artificial intelligence techniques, empowering states to derive meaningful intelligence and knowledge from this data reservoir [49].

Data assumes significant importance for cyber power and is often likened to the "new currency" or "new oil" in the digital age. It plays a pivotal role in the development of Artificial Intelligence (AI) technologies, as the underlying logic of AI systems relies on vast volumes of data for learning, comprehension, decision-making, and performance enhancement [49]. The abundance of data correlates with reduced errors in AI systems, making data ownership and accessibility crucial for advancing AI services within a country. The possession and utilization of data have substantial implications for a nation's cyber intelligence, surveillance, and cyber offensive/defensive operations. A country's ability to own and manage data can significantly impact its cyber capabilities and prowess. By examining a country's performance in these areas, valuable insights can be gleaned regarding its proficiency or limitations in data collection and ownership [50].

Similarly, in cyber surveillance, data ownership is instrumental in monitoring and detecting potential cyber threats or illicit activities within a country's digital infrastructure. Surveillance activities heavily rely on data streams to identify suspicious patterns or behaviors, thereby bolstering the nation's cyber resilience and situational awareness [51].

Regarding cyber offensive and defensive operations, data plays a critical role in enhancing the efficacy of these activities. Governments can leverage data-driven intelligence to formulate offensive cyber operations, targeting specific adversaries or vulnerabilities. On the defensive front, possessing robust data resources allows for proactive measures in fortifying cyber defenses and responding to emerging threats promptly [52, p. 32].

Data ownership is a cornerstone of a country's cyber power, impacting various facets of its cyber capabilities. Access to vast and diverse datasets fuels the development of AI technologies and strengthens a nation's cyber intelligence, surveillance, and offensive/defensive operations [10]. Evaluating a country's performance in these domains provides valuable insights into its ability to collect, manage, and utilize data effectively, ultimately contributing to its overall cyber power and resilience.

Nevertheless, as the PTT contends that while the population, including the internet population, constitutes a vital resource for national power, it is not the sole determinant [39]. Similarly, in cyberspace, although a high internet population and data are essential objectives for a rational state, they do not encompass the entirety of its pursuits. To comprehensively grasp the dynamics of cyber power, examining a country's performance in its digital economy is imperative. Assessing a country's digital economy offers valuable insights into its ability to effectively harness its resources, such as the internet population and data, to attain digital economic competitiveness.

5.2. Cultivation of a Robust Digital Economy

The global economy is undergoing a profound transformation driven by the rapid advancement and widespread adoption of information and communication technologies (ICTs). Notably, the proliferation of digital data over the internet has been accompanied by the rise of significant technologies such as big data analytics, artificial intelligence (AI), cloud computing, and novel business models. The continuous expansion of internet-connected devices and users and the increasing integration of value chains through digital means further underscores the escalating significance of digital data and technologies [53]. Consequently, the ability to access and leverage data effectively, transforming it into digital intelligence, assumes critical importance in determining the competitiveness of states in the contemporary economic landscape.

The ongoing digitalization process in the global context has led to the emergence of the digital economy, which, at its nascent stage, lacks a universally accepted definition. In the late 1990s, initial analyses of the digital economy primarily centered on the adoption of the Internet and its economic implications [54]. As Internet usage continued to expand, subsequent reports from the mid-2000s onward examined the factors that could facilitate the growth and development of the internet economy.

The digital economy can be defined as a subset of the overall economic output that stems from the utilization of digital technologies and is structured around business models primarily centered on digital goods or services [43]. However, other scholars present a more comprehensive perspective, considering the digital economy as the total economic output derived from diverse digital elements.

These digital inputs encompass various aspects, including digital skills, equipment, digital goods, ICT exports, and digital services

utilized in production. This broader definition allows for a more comprehensive examination of a country's digital economy, whether in the context of its domestic or international dimensions. By analyzing a nation's performance across these digital inputs, valuable insights can be gleaned regarding the economic output (digital economy) generated from these digital resources [43].

For several significant reasons, the digital economy plays a pivotal role in shaping a country's cyber power. First, it serves as a driving force behind technological advancements and innovations in cybersecurity and cyber technologies [55]. The continuous growth of the digital economy necessitates the development of sophisticated cybersecurity capabilities, including robust threat detection and incident response systems.

Secondly, establishing a strong digital economy requires the implementation of sophisticated cyberinfrastructure that supports various cyber operations and services. This infrastructure forms the foundation for effective cyber governance and management [53].

A flourishing digital economy enhances a country's economic competitiveness and global influence in the cyber domain. A strong presence in the digital economy elevates a nation's reputation and standing in the international cyber landscape.

Overall, a thriving digital economy serves as the backbone of a nation's cyber strength and resilience, enabling it to effectively navigate the complexities and challenges of the cyber domain [55].

5.3. Cultivation of a High Degree of Cyber Political Capacity

The objectives pertinent to a rational state's interests in cyberspace encompass data ownership, information management, cybersecurity, offensive capabilities, cyberinfrastructure, and economic aspects of cyber power. However, a comprehensive analysis of cyber power requires the consideration of additional dimensions. Analogous to the Power Transition Theory's emphasis on political capacity as the government's ability to effectively mobilize resources and achieve national objectives, the realm of cyberspace also demands a high degree of cyberpolitical capacity [39].

Cyber-political capacity in cyberspace pertains to a state's capability to wield cyber resources and technologies to achieve its strategic goals and policy objectives. This includes the effective governance and management of cyber operations, cyber policies, and cyber

strategies at the national level. States with robust cyber-political capacities can leverage their cyber capabilities to assert their interests, influence the global cyber landscape, and safeguard their national security in cyberspace.

Domestically, cyber political capacity involves a country's ability to promptly and effectively formulate policy decisions on cyber-related matters. This includes establishing comprehensive cyber strategies, laws, and regulations that optimize the use of cyber resources for advancing national interests in the international cyberspace domain. A state's ability to effectively govern its cyber activities is fundamental to its capacity to project power internationally. Strong domestic cyber political capacity ensures that the state's cyber infrastructure is resilient, its policies are forward-thinking, and its workforce is skilled and adaptable to emerging cyber threats and opportunities. This internal governance forms the backbone of a country's overall cyber power, enabling it to respond rapidly and efficiently to cyber challenges.

On the international stage, cyber political capacity extends to a country's ability to influence the formulation of global cyber norms, regulations, principles, and standards that align with national interests. This aspect of cyber capacity is closely related to the broader concept of international cyber governance. A nation with significant international cyber-political capacity can shape the international cyber domain's rules, thereby exerting influence over how cyberspace is used, regulated, and protected. Effective participation in international cyber policymaking forums, alliances, and coalitions is crucial. Countries with strong international cyber-political capacities can push for norms and regulations that favor their strategic interests, promote global stability, and prevent cyber conflicts.

The importance of cyber-political capacity cannot be overstated. This capacity is a crucial enabler for a state to achieve and maintain cyber power. Cyber political capacity encompasses the strategic governance and management of a state's cyber resources, policies, and operations, aligning them with national objectives. Without effective governance and strategic management, even states with significant data resources and a robust digital economy may find their cyber power potential constrained. A lack of coherent strategy can lead to disjointed efforts, inefficiencies, and vulnerabilities that adversaries could exploit.

Conversely, states with robust cyber-political capacities can maximize the utility of their cyber assets. Effective governance ensures

that cyber activities are coherent, well-coordinated, and strategically aligned with national objectives. This alignment facilitates the seamless integration of cyber capabilities into broader national security and economic strategies, amplifying the impact of cyber initiatives. For instance, comprehensive cyber strategies can enhance defensive measures against cyber threats, ensure critical infrastructure protection, and bolster the state's ability to conduct offensive cyber operations when necessary.

Moreover, the ability to shape international cyber norms and policies in an interconnected world provides a strategic advantage. States with substantial cyber political capacity can actively participate in international forums, influence the development of global cyber norms, and advocate for policies that promote their strategic interests. This ability to shape the international cyber environment allows states to create a favorable setting for their cyber operations and defend against potential adversaries. By promoting norms such as state sovereignty in cyberspace, the prohibition of certain types of cyber-attacks, or the protection of critical infrastructure, states can contribute to a more stable and secure international cyber landscape.

In addition, robust cyber-political capacity enables states to build and sustain strategic alliances and partnerships. These relationships can enhance a state's cyber capabilities through shared intelligence, collaborative defense initiatives, and coordinated responses to cyber threats. For example, alliances such as NATO have recognized cyberspace's significance as a warfare domain, and member states benefit from collective defense measures and shared resources to bolster their individual and collective cyber defenses.

In conclusion, while possessing state cyber capacity is integral to achieving state cyber power, realizing robust state cyber capacity requires substantial data resources and a strong digital economy. Thus, the three elements of cyber power, data resources, economic strength, and cyber political capacity are mutually reinforcing and complementary. A state's cyber-political capacity is pivotal in this triad, enabling effective utilization and governance of cyber resources to project power, protect national interests, and influence the global cyber order.

Cyber political capacity ensures that a state's cyber efforts are strategically guided, well-coordinated, and effectively implemented, thereby maximizing the potential of its cyber assets. This capacity strengthens national security and economic resilience and provides

a platform for influencing international cyber policies and norms, creating a favorable global environment for the state's cyber activities. In essence, robust cyber political capacity is the linchpin that enables states to harness their cyber resources fully, navigate the complexities of the digital age, and maintain a competitive edge in the international arena.

6. Conclusion

This study underscores the profound significance of cyberspace in contemporary global politics and the necessity of understanding cyber power within the framework of traditional IR theories. The research aims to fill a critical gap in the existing literature by applying PTT to cyberspace, considering the state as a rational and unitary actor. By integrating PTT with the rational actor model and defining cyber power based on specific objectives, this study offers a novel perspective on the assessment and categorization of cyber power.

The primary objective of this research is to define cyber power and propose a metric for its assessment, analogous to PTT's approach to evaluating national power. This involves a comprehensive analysis of cyber power by breaking it down into three core components: data resources, digital economic strength, and cyber political capacity. These elements form the basis for assessing state cyber power and understanding the hierarchical structure of states in cyberspace.

The study employs a methodological framework borrowed from PTT to achieve these objectives. It uses the rational actor model, which assumes that states act logically and strategically to maximize their interests in cyberspace. By taking the state as a unitary actor, the research simplifies the complex interactions within cyberspace, allowing for a clearer analysis of state behavior and cyber power dynamics. Furthermore, the study defines cyber power based on specific objectives, such as data ownership, information management, cybersecurity, offensive capabilities, cyberinfrastructure, and the economic aspects of cyber power.

The application of PTT to cyberspace reveals a nuanced understanding of cyber power. PTT emphasizes the importance of a comprehensive assessment of national power, traditionally measured through economic, military, and demographic indicators. This translates to a tripartite model comprising data resources, digital economic strength, and cyber political capacity in the cyber domain.

Each of these elements is crucial for a state to project power and protect its interests in cyberspace.

Data resources form the backbone of cyber power, enabling states to gather, analyze, and leverage information for strategic purposes. A strong digital economy provides the financial and technological infrastructure to support advanced cyber capabilities. However, the linchpin of this triad is cyber-political capacity. This dimension pertains to the state's ability to effectively govern and manage its cyber resources, craft coherent cyber policies, and engage in international cyber diplomacy. States with robust cyber-political capacities can coordinate their cyber activities, safeguard national security, and influence global cyber norms to create a favorable environment for their operations.

The hierarchical model of cyber power proposed in this study categorizes states into four distinct groups: global cyber leaders, cyber great powers, cyber-dependent powers, and non-cyber powers. This classification reflects the varying degrees of cyber capability and influence among states, providing a structured framework for analyzing the global cyber landscape. Global cyber leaders, or in other words, the most dominant state in cyberspace, exemplified by the United States, possess comprehensive cyber capabilities and play a central role in shaping international cyber policies. Cyber great powers, such as the European Union, China, and Russia, hold substantial influence but exhibit different levels of satisfaction with the existing cyber order, influencing their international cyber strategies. Cyber-dependent powers, while having certain cyber capabilities, rely significantly on external technologies and face vulnerabilities in cybersecurity. Non-cyber powers, with limited internet penetration and digital infrastructure, struggle to participate meaningfully in the global cyber arena.

In addition to the contribution of this study to the literature on cyberspace and IR, important clarification is also necessary regarding the scope and intent of this study. While Power Transition Theory traditionally deals with the dynamics of power shifts between states, this research does not focus on the concept of "power transition" within cyberspace. Instead, its primary aim is to apply PTT's national power model to the cyber domain to define and measure cyber power, thereby establishing a hierarchical order of states in cyberspace. This initial step is critical as it lays the groundwork for future studies to explore the dynamics of power transitions once cyber power has been accurately measured using the proposed

model. Some might see this as a limitation of the study, and critics might argue that applying PTT to cyberspace without directly exploring "transition" dynamics is premature. However, this study is a preliminary effort to introduce an IR perspective on the definition and assessment of cyber power. By borrowing PTT's national power definition and assessment model, this research establishes the relevance of traditional IR theories to the cyber domain. This foundational work is crucial as it sets the stage for future analyses of power transitions in cyberspace, which can only be thoroughly examined once cyber power has been accurately assessed by the model introduced in this study.

In conclusion, while possessing state cyber capacity is integral to achieving state cyber power, realizing robust state cyber capacity requires substantial data resources and a strong digital economy. The three elements of cyber power, data resources, digital economic strength, and cyber political capacity, are mutually reinforcing and complementary. A state's cyber political capacity plays a pivotal role in this triad, enabling effective utilization and governance of cyber resources to project power, protect national interests, and influence the global cyber order. By applying traditional IR theory to the domain of cyberspace and demonstrating its applicability, this research addresses a significant gap in the existing literature. It also puts forward an innovative model for assessing cyber power and provides valuable insights into the hierarchical structure of states within cyberspace. These contributions are substantial, offering a new lens through which to understand global cyber governance and geopolitical relations in this emerging and critical domain.

References

[1] M. Carr, *US power and the Internet in international relations: The irony of the information age*. Basingstoke and New York: Palgrave Macmillan, 2016, doi: 10.1057/9781137550248.

[2] A.H. Morrison, "An impossible future: John Perry Barlow's 'Declaration of the Independence of Cyberspace,'" *New Media and Society*, vol. 11, no. 1–2, pp. 53–71, 2009, doi: 10.1177/1461444808100161.

[3] R. Creemers, "Governing cyberspace: behavior, power and diplomacy," in *Governing Cyberspace: Behavior, Power and Diplomacy*, D. Broeders, B. Van den Berg, Eds., London: Rowman & Littlefield, 2020, pp. 116–151.

[4] Z. Hongren, "Strategic stability in cyberspace: a chinese view," *China Quarterly of International Strategic Studies*, vol. 5, no. 1, pp. 81–95, 2019, doi: 10.1142/S2377740019500088.

[5] J. Nocetti, "Contest and conquest: Russia and global internet governance," *International Affairs*, vol. 91, no. 1, pp. 111–130, 2015, doi: 10.1111/1468-2346.12189.

[6] H. Ebert, T. Maurer, "Contested cyberspace and rising powers," *Third World Quarterly*, vol. 34, no. 6, pp. 1–22, 2013, doi: 10.1080/01436597.2013.802502.

[7] J. van Haaster, "Assessing cyber power," in *2016 8th Internatıonal Conference on Cyber Conflıct*, M. V. N.Pissanidis, H.Rõigas, Eds., Tallınn: NATO CCD COE Publications, 2016, pp. 85–90.

[8] N. Inkster, "Measuring military cyber power," *Survival*, vol. 59, no. 4, pp. 27–34, 2017, doi: 10.1080/00396338.2017.1349770.

[9] M. Willett, "Assessing cyber power," *Survival*, vol. 61, no. 1, pp. 85–90, 2019, doi: 10.1080/00396338.2019.1569895.

[10] D.J. Betz, T. Stevens, "Power and cyberspace," *Adelphi Series*, vol. 51, no. 424, pp. 35–54, 2011, doi: 10.1080/19445571.2011.636954.

[11] J.S. Nye, "Cyber Power," *Harvard Kenddy School Belfer Center for Scıence and Internatıonal Affaırs*, no. 6, pp. 2–4, 2015, doi: 10.12816/0022579.

[12] G. Rose, "Neoclassical Realism and theories of foreign policy," "https://www.cambridge.org/core/journals/world-politics" *World Politics*, vol. 51, no. 1, pp. 144–172, 2010.

[13] T. Dunne, M. Kurki, S. Smith, Eds., *International Relations Theories Discipline and Diversity*, 1st ed. London: Oxford University Press, 2007.

[14] J.S. Nye, *Soft Power and Great-Power Competition: Shifting Sands in the Balance of Power Between the United States and China*. MA Singapore: Springer. doi: https://doi.org/10.1007/978-981-99-0714-4.

[15] E.L. Armistead, "Suggestions to measure cyber power and proposed metrics for cyber warfare operations (cyber deterrence/cyber power)," *2016 IEEE International Conference on Cyber Conflict, CyCon U.S.* 2017, doi: 10.1109/CYCONUS.2016.7836610.

[16] J. Arquilla, D. Ronfeldt, "Cyberwar is coming," *Rand Corporation*, 1993. Available: https://www.rand.org/pubs/reprints/RP223.html [Accessed: July 25, 2024].

[17] M.C. Libicki, "Information war, information peace," *Journal of International Affairs*, vol. 51, no. 2, pp. 411–428, 1998.

[18] M. Castells, *The Rise of the Network Society*. New York: Blackwell Pub, 1996. doi: 10.1002/9781444319514.

[19] S. Sassen, *Globalization and Its Discontents Essays on the New Mobility of People and Money*. New York: The New Press, 1999.

[20] R.J. Keohane, J. Nye, *Power and Interdepence*. 1st ed. New York: Pearson, 1988.

[21] J.N. Rosenau, J.P. Singh, Eds., *Information Technologies and Global Politics The Changing Scope of Power and Governance*. New York: State University of New York Press, 2002.

[22] H. Nissenbaum, "Where computer security meets national security," *Ethics and Information Technology*, vol. 7, no. 1, pp. 61–73, 2005, doi: 10.1007/s10676-005-4582-3.

[23] A. Chadwick, *Internet Politics: States, Citizens, and New Communication Technologies*, 1st ed. London: Oxford University Press, 2006.

[24] R. Deibert, R. Rohozinski, "Control and subversion in Russian cyberspace," in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, R. Deibert, J. Palfrey, R. Rohozinski, J. L. Zittrain, Eds., London: The MIT Press, 2010, pp. 15–34. doi: https://doi.org/10.7551/mitpress/8551.001.0001.

[25] N. Choucri, *Cyberpolitics in International Relations*. London: The MIT Press, 2012. doi: 10.7551/mitpress/7736.003.0009.

[26] J.R. Lindsay, "Stuxnet and the limits of cyber warfare," *Security Studies*, vol. 22, no. 3, pp. 365–404, Jul. 2013, doi: 10.1080/09636412.2013.816122.

[27] A. Venables, S.A. Shaikh, J. Shuttleworth, "The projection and measurement of cyberpower," *Security Journal*, vol. 30, no. 3, pp. 1000–1011, 2017, doi: 10.1057/sj.2015.35.

[28] D. Brizhinev, N. Ryan, R. Bradbury, "Modelling hegemonic power transition in cyberspace," *Complexity*, vol. 2018, pp. 1–13, 2018, doi: 10.1155/2018/9306128.

[29] R.L. Tammen, *Power transition: Strategies for the 21st century*, 1st ed. New York: CQ Press, 2000.

[30] W. Kim, S. Gates, "Power transition theory and the rise of China," *International Area Studies Review*, vol. 18, no. 3, pp. 219–226, 2015, doi: 10.1177/2233865915598545.

[31] M. Bussmann, J. R. Oneal, "Do hegemons distribute private goods?: A test of power-transition theory," *Journal of Conflict Resolution*, vol. 51, no. 1, pp. 88–111, 2007, doi: 10.1177/0022002706296178.

[32] R.N. Lebow, B. Valentino, "Lost in transition: a critical analysis of power transition theory," *International Relations*, vol. 23, no. 3, pp. 389–410, 2009, doi: 10.1177/0047117809340481.

[33] R. L. Tammen, J. Kugler, D. Lemke. (Oct. 26, 2017). Foundations of Power Transition Theory. [Online]. Available: https://oxfordre.com/politics/display/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-296?product=orepol. [Accessed: Apr. 04, 2021].

[34] W. Kim, S. Gates, "Power transition theory and the rise of China," *International Area Studies Review*, vol. 18, no. 3, pp. 219–226, 2015, doi: 10.1177/2233865915598545.

[35] Y. Akdag, "The likelihood of cyberwar between the United States and China: A neorealism and power transition theory perspective," *Journal of Chinese Political Science*, vol. 24, no. 2, pp. 225–247, 2019, doi: 10.1007/s11366-018-9565-4.

[36] M. Bey, "Great powers in cyberspace: the strategic drivers behind US, Chinese and Russian competition," *International Conference on Cyber Conflict*, vol. 126, no. 1, pp. 1–7, 2019.

[37] T. Ray, "The quest for cyber sovereignty is dark and full of terrors," *ORF*. [Online]. Available: https://www.orfonline.org/expert-speak/the-quest-for-cyber-sovereignty-is-dark-and-full-of-terrors-66676/. [Accessed: Apr. 04, 2021].

[38] T. Woodhouse, "Alliance for affordable internet," 1BC. [Online]. Available: https://a4ai.org/report/2021-affordability-report/#i-acknowledgements.2021. [Accessed: Dec. 23, 2023].

[39] S. Han, "China's pursuit of peaceful power transition: a case of ICT (Information and Communications Technologies) standard setting," *International Area Studies Review*, vol. 12, no. 3, pp. 27–42, 2009, doi: 10.1177/223386590901200302.

[40] A. Kosenkov, "Cyber conflicts as a new global threat," *Future Internet*, vol. 8, no. 3, 2016, doi: 10.3390/fi8030045.

[41] R.B. Andres, „The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, D. S. Reveron, P. Jagoda, H. Lin, Eds., Washington DC: Georgetown University Press, 2012, pp. 89–104.

[42] E. Gartzke, "The myth of cyberwar bringing war in cyberspace back down to Earth," *International Security*, vol. 38, no. 2, pp. 41–73, 2013, doi: 10.1162/ISEC_a_00136.

[43] J. Zhang *et al.*, "The impact of digital economy on the economic growth and the development strategies in the post-COVID-19 era: evidence from countries along the 'Belt and Road,'" *Frontiers in Public Health*, vol. 10, no. May, pp. 1–17, 2022, doi: 10.3389/fpubh.2022.856142.

[44] M. Carr, "Power plays in global internet governance," *Millennium: Journal of International Studies*, vol. 43, no. 2, pp. 640–659, 2015, doi: 10.1177/0305829814562655.

[45] J.J. van Vuuren, L. Leenen, "A model for measuring perceived cyberpower," Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018, 2018, pp. 320–327.

[46] N. Inkster, *China's Cyber Power*, 1st ed. Oxon: Taylor & Francis, 2016. Available at: https://www.routledge.com/Chinas-Cyber-Power/Inkster/p/book/9781138211162 (Accessed: Jan. 20, 2023).

[47] L. Tsui, "The panopticon as the antithesis of a space of freedom: Control and Regulation of the Internet in China," *China Information*, vol. 17, no. 2, pp. 65–82, 2003, doi: 10.1177/0920203X0301700203.

[48] R.Á. Pinto, "Digital sovereignty or digital colonialism?," *International Journal on Human Rights*, vol. 15, no. 27, pp. 15–27, 2018.

[49] S. Hoffmann, S. Bradshaw, E. Taylor, "Networks and geopolitics: How great power rivalries infected 5G," *Oxford Information Labs*, pp. 37, 2019.

[50] F.C. Domingo, "Conquering a new domain: Explaining great power competition in cyberspace," *Comparative Strategy*, vol. 35, no. 2, pp. 154–168, 2016, doi: 10.1080/01495933.2016.1176467.

[51] T. Rid, B. Buchanan, "Attributing cyber attacks," *Journal of Strategic Studies*, vol. 38, no. 1–2, pp. 4–37, 2015, doi: 10.1080/01402390.2014.977382.

[52] S.W. Lonergan, "Cyber power and the international system," Columbia University, 2017. doi: 10.7916/D88D07PH.

[53] UNCTAD, "Digital Economy Report 2021- Cross-border data flows and development: for whom the data flow," New York, 2021.

[54] Q. Meng, M. Li, "New economy and ICT development in China," *Information Economics and Policy*, vol. 14, no. 2, pp. 275–295, 2002, doi: 10.1016/S0167-6245(01)00070-1.

[55] Centre for Strategic and International Studies, *G20 Toolkit for Measuring Digital Skills and Digital Literacy: Framework and Approach*. [Online]. Available: https://www.csis.or.id/publication/g20-toolkit-for-measuring-digital-skills-and-digital-literacy-framework-and-approach/ (Accessed Apr. 02, 2023).