CARTA INTERNACIONAL
ASSOCIAÇÃO BRASILEIRA DE RELAÇÕES INTERNACIONAIS

ISSN 2526-9038

Measuring Influence in cyberspace: A Social Network Analysis application for investigating cyber power dynamics

Mensurando Influência no ciberespaço: Uma aplicação de Social Network Analysis *para investigação das dinâmicas do poder cibernético*

Medición de la influencia en el ciberespacio: una aplicación del Social Network Analysis *para investigar la dinámica del poder cibernético*

10.21530/ci.v17n2.2022.1296

Victor Andrês Veloso Cavadas[1]
Marislei Nishijima[2]

Abstract

Infrastructure control is considered a critical resource for the power projection of nations. In this sense, one of the most important infrastructures in the virtual environment of the Internet, or cyberspace, is the submarine cables. However, the literature points to difficulties in objectively measuring the capabilities that each actor has in this ecosystem. Thus, we use Social Network Analysis to assess the degree of importance of Europe, BRICs, and the United

1 Mestrando em Ciências pelo programa de pós-graduação em Relações Internacionais pelo Instituto De Relações Internacionais da Universidade de São Paulo (IRI-USP). (vvelosocavadas@gmail.com). **ORCID: https://orcid.org/0000-0001-6465-7640**.

2 Doutora em Teoria Econômica pela Universidade de São Paulo. Professora Associada do Instituto de Relações Internacionais da Universidade de São Paulo, São Paulo, Brasil. (marislei@usp.br). **ORCID: https://orcid.org/0000-0003-1162-7987**.

Artigo submetido em 22/08/2022 e aprovado em 2/10/2022.

States actors regarding the potential access to flows of information from the submarine Internet backbones. The results suggest that the United States has the hegemony power but it is losing relative positions to China and Europe.

Keywords: Submarine Cables; Social Network Analysis; Cyberspace; Cyber Power.

Resumo

O controle de infraestrutura é considerado um recurso crítico para a projeção de poder das nações. Nesse sentido, uma das infraestruturas mais importantes no ambiente virtual da Internet, ou ciberespaço, são os cabos submarinos. No entanto, a literatura aponta dificuldades em mensurar objetivamente as capacidades que cada ator possui nesse ecossistema. Assim, utilizamos a *Social Network Analysis* para avaliar o grau de importância dos atores da Europa, dos BRICs e dos Estados Unidos quanto ao potencial de acesso aos fluxos de informação dos *backbones* submarinos da Internet. Os resultados sugerem que os Estados Unidos têm o poder de hegemonia, mas estão perdendo posições relativas para China e Europa.

Palavras-Chave: Cabos Submarinos; *Social Network Analysis*; Espaço Cibernético; Poder Cibernético.

Resumen

El control de la infraestructura se considera un recurso crítico para la proyección de poder de las naciones. En este sentido, una de las infraestructuras más importantes en el entorno virtual de Internet, o ciberespacio, son los cables submarinos. Sin embargo, la literatura señala dificultades para medir objetivamente las capacidades que tiene cada actor en este ecosistema. Por lo tanto, utilizamos el análisis de redes sociales para evaluar el grado de importancia de los actores europeos, BRIC y estadounidenses en términos del potencial para acceder a los flujos de información de las redes troncales submarinas de Internet. Los resultados sugieren que EE. UU. tiene poder hegemónico, pero está perdiendo posiciones relativas frente a China y Europa.

Palabras clave: Cables Submarinos; Análisis de redes sociales; Ciberespacio; Poder cibernético.

Introduction

Cyberspace has been an important theme in States' defense and security strategies in recent decades. Although scientific production and the formulation of public policies are increasingly present, the area still finds obstacles in defining core concepts such as cyberspace and cyber power. The absence of a standard definition of these terms hampers the exchange of studies and methodologies and the debate between nations on how to deal with the challenges imposed by the new dynamics of this domain (Libicki 2012) .

It is common and quite easy to demonstrate that a relatively small number of United States-based companies such as Apple, Alphabet (Google), Meta (Facebook), and Amazon have accumulated dominance over such applications and services over time. Indeed, around the world, in the past half-decade alone there have been well over one hundred public inquiries and regulatory examinations that aim to develop a new generation of Internet services and content regulations to address these realities. Moreover, the dominance of Google in search and Facebook with respect to social network services has also proven to be stubbornly persistent, and this, too, has been the subject of a string of legal cases and regulatory developments that aim to reign in these companies' market dominance and anti-competitive practices, while establishing new modes of regulation and standards of the public interest for the Internet-centric, digital media environment of the 21st Century (U.S. 2021)

For example, according to Winseck (2017), the hegemony of the United States over the "physical layer" of cyberspace has steadily declined over the last two decades relative to the European Union and BRICS (Brazil, Russia, India, China, and South Africa) countries. The author locates the power dynamics of cyberspace by framing the possession of physical and informational infrastructures and uses the concentration of ownership of critical infrastructures such as content distribution networks (CDN), Autonomous Systems Numbers (ASN), and Internet exchange points (IXP), and the submarine cables that make up the Internet backbone, to measure the extent of power possessed by different actors, including nation-states and changes in the distribution of power over time.

Such studies are important because, as Susan Strange (1975) observed, the control of communication structures—alongside control over security, production and finance—is one of the defining elements of structural power: namely, the ability to create and enforce the institutional context and rules within which

other actors must operate (Haggart 2017). In this line, Winseck (2017) agrees that the United States and the major international Internet services companies domiciled there are hegemonic in terms of applications and services (e.g. operating systems (e.g. iOS and Android), search engines (e.g. Google), social networks (e.g. Facebook), etc.). However, the same does not hold true for the physical, or material, infrastructures that underpin the applications and services made available over the Internet (Winseck 2017). Actually, the authors' analysis concludes that the hegemony of the United States over the "physical layer" of cyberspace has steadily declined over the last two decades compared to the European Union and BRICS (Brazil, Russia, India, China, and South Africa) countries.

Building on Winseck's (2017) conceptual bases, this paper employs Social Network Analysis (SNA) methods to measure the distribution of infrastructure ownership among selected countries (United States, BRICS, and some European countries) between 2011-2017. According to Freeman (1978) and Scott and Carrington (2011), the methodology provides a quantitative analysis of the power and hierarchical organization of control in communications networks by examining the physical links in that network, its connection points, and the capacity of a network. Thus, it involves examining the physical submarine cable communication links that exist between countries—the overwhelmingly dominant mode of connecting countries worldwide, given that they account for roughly between 95% and 99% of Internet traffic in 2020—the location of the points where these connections occur and the capacity of each of these communication links. We study the distribution of the network of overseas cables among a panel of selected countries and their changes in the relative capacity to exercise power and control over international Internet traffic.

The SNA allows us to chart changes in the relative dominance of different countries and regions with respect to international Internet traffic over time and uses a precise and quantitatively rigorous approach. In addition, we use the information on all central submarine cables to make the calculations, despite focusing the analysis on the relations between the United States, selected European countries, and BRICS countries. In this sense, the method is robust to potential changes in other countries. The main use of this tool is to measure the potential capacity for countries to exercise power and control over the international Internet based on systematic observations about the evolution of submarine cables belonging to States over time and across space and each country's information transmission capacity. This context matters since the structures organized as a

network are complex and need social network methods, such as the SNA, which allows for measuring the power relations among countries. The SNA can also bring information on the links' capacity for relationships between numerous and different actors. In this sense, the analysis allows us to assess which country is connected to and with how much force. Each country represents a point of the network, with each link labeled with a strength of this connection. The measure of linking force is illustrated by the sum of the potential flow of data (GB/s) between each country.

After the calculations, we compared the results with Winseck's (2017) article and reached similar general conclusions. This similarity strengthens the use of the SNA as a potential tool for robust quantitative analyses. In addition, SNA can also analyze a context from a network perspective and get closer to the form of these dynamics in cyberspace. Essentially, SNA measures the power of an individual agent through their connections in a relative way, offering a fuller comprehension of the environment in which an agent is involved, a country in our case. For instance, the method allows comparing different countries' blocs in a whole and relational context, keeping the same data as a resource for other works in the future since the connections are peer-to-peer.

The rest of the paper is organized as followed. The next section reviews the literature relevant to our analysis, while section three describes the methods we use and the data that we have gathered. Section four presents and discusses the results of our research, while the last section considers the theoretical and substantive implications of our findings in terms of mapping and understanding changes in the geopolitics and political economy of the Internet and the nature of power and control in international communications.

Cyber Power and Critical Internet Infrastructures

The choice to use physical infrastructures as an object of study provides part of a solution to the impasse of consensus on the definition of cyberspace and consequently of the potential power that acts in these areas. The uncertainty lies in which elements should compose cyberspace and how each of the elements included in this definition—or not—confer the ability to exercise power and control over both the Internet itself and the traffic, services, and applications made available over the Internet (Libick 2012).

The problem of defining cyberspace has long preoccupied those who work in security studies. Three decades ago and just as the commercial Internet was taking off, for example, Arquilla and Ronfeldt (1993) described cyberspace as "the realm" formed by a three-fold arrangement of hardware infrastructures, software, and the flow of information involved. Kuehl (2009) delineates cyberspace as an operational domain whose distinctive and unique character is shaped by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected information and communication technology (ICT)-based systems and their associated infrastructure. Similar to Arquilla and Ronfeldt's definition, authors like Ventre (2012), Libick (2012), and Kurbalija (2017) describe cyberspace as composed of three layers; physical, semantic, and syntactic. The physical layer comprises the critical infrastructures that support the existence of information flows, the semantics refers to the information flow itself, and the syntactic is illustrated by the protocols by which machines interact with each other. Choucri and Clark (2018) added a fourth layer to the definition of cyberspace by including the people who use the Internet, since social interactions define the directions of information flows and determine the success or failure of particular cyberspace technologies and applications, thus altering its power dynamics.

The United States Department of Defense defines cyberspace as a global domain within the information environment that consists of interdependent networks of information technology infrastructures and resident data (US 2021). The European Union Cyber Security Agency (ENISA) defines it as containing tangible (physical infrastructure) and intangible (information and data) elements (Tirtea 2017). NATO also defines cyberspace as composed of a network of computer systems and telecommunication networks, in addition to the information that circulates through them (Costigan et al. 2016). It is observed that, in all these definitions, physical and informational infrastructures are characterized as complementary in the delineation of cyberspace and the power dynamics intrinsic to this domain. In other words, each of these definitions places as much weight—or more—on the actual material infrastructure of the Internet as they do on the information, applications, and services made available over the Internet.

Nonetheless, according to Betz and Stevens (2011), all these definitions remain vague and underspecified. The sources of this conceptual problem from a methodological point of view are two-fold. First, the available data needed to get a good empirical grasp on the material infrastructural elements and the

informational dimension of the Internet are difficult to obtain because they are scarce and extremely expensive to procure when available. Second, how control over communication confers power on the different actors involved in the ownership, operation, and governance of the Internet is difficult to theorize or document. This paper tries to overcome these challenges in ways that will become evident in the pages ahead.

The main difficulty rests on the fact that this domain is, fundamentally, a human creation composed of the socio-technical arrangements of those who built it. Furthermore, these arrangements are in constant dispute and forever undergoing changes that are shaped by political and economic processes. In this sense, the Internet is not a fixed thing but a steadily evolving system of relationships subject to periodic step changes that differentiate more recent iterations from past phases of development. Moreover, the actors in the overarching network of networks also experience the reality that their own positions and capabilities are dependent on the relational nature and conditions of the overall system within which they are situated and act. Consequently, each actor's power is a reflexive relationship, and the capabilities/possibilities structuring these relationships are decisive factors in determining each actor's own power. In addition, as developments in the Internet over time reduce the temporal and spatial barriers between actors while increasing the number of actors dynamically involved overall, each actor tends to be affected by emergent forms of power that had previously been more limited in time, space and physical capabilities, or invisible altogether. Given the complexity of these processes and their dynamically evolving nature, it should not be surprising that it is extremely difficult, to say the least, to assess different actors' capacity to exercise power and influence outcomes.

It is also important to understand what we mean by power in this context. To do so, we draw on the work of Steven Lukes (1975) and Susan Strange. According to Lukes (1975), power comes in three forms. The first is the "instrumental power', or the ability of one actor to get another actor to do what they want or desire, even if it is not in the latter's best interest. As in a fistfight or a game, this kind of power is visible, and winners and losers are easy to see. The second form of power, which underpins this paper, is what the author calls "structural power". Structural power is the ability of an actor, or a group of actors working in concert with one another, to set and institutionalize the rules by which all actors must abide. The ability to make the rules by which others must adhere, and to institutionalize and enforce those rules, can be done by single actors but often

involves cooperation among actors, as in a multilateral and multistakeholder model of international relations or Internet governance, for example. In some contexts, those who abide by the rules created, maintained, and enforced by others will only be dimly aware of the rules and institutional arrangements that they must comply with and which are, even if subtly and in the background, structuring their behavior (and their prospects). The third face of power is *ideological power*, the set of ideas and beliefs—often tacitly accepted and held—that underpins actors' belief in and the legitimacy of a set of social and political arrangements. For example, we can point to the idea of the 'free and open Internet' a belief system that has attended discussions and the governance of the Internet for much of the last three decades. This paper relies mainly on the concept of structural power.

In addition to the structural power concept of Lukes (1975), we can cite the 1975 study of the international political economist Susan Strange. Strange (1975) made this concept of power a central piece to her analysis of the international financial system and the international political economy that she saw as being dominated by the United States at the time of her writing in the latter decades of the 20th Century. According to the author, structural power is the capacity of an actor (or, less so, a group of actors) to determine the institutional arrangements and regime of rules that underpin and frame the international political economy within which other states, their institutions, and companies must operate. She proposes that the evolution of information formats and control over knowledge are absolutely critical to the formation and maintenance of structural power and must be investigated since, whoever controls the "knowledge structure" has the potential capacity to influence the ownership and control of the infrastructures and systems through which this knowledge, money, and authority is transmitted. The power derived from the structure of knowledge comes as much from what is believed by actors as from who controls the actual channels in which beliefs are communicated or filtered (May 1996).

Winseck (2017) and Haggart (2017) draw on the theorization of structural power and the knowledge structure upon which it rests that Strange (1975) developed to study geopolitics, political economy, and regulation of the Internet. Winseck (2017), in particular, focuses on communication infrastructures—both historical in nature, such as telegraph and wireless networks in the late-19th and early-20th Centuries and contemporary, as in the worldwide Internet—as objects of study and with an eye to understanding baseline questions about who owns and controls the Internet. That focus is also in line with Betz and Stevens (2011),

who take up similar questions but with a more specific focus on how control over Internet resources affects questions of national security.

A case that illustrates how the structure of knowledge can be materialized is the revelations of former US National Security Agency (NSA) agent Edward Snowden. In 2013, Snowden revealed the massive global surveillance apparatus orchestrated by the NSA in conjunction with other intelligence agencies. Among the various programs, the upstream collection exemplifies how infrastructure ownership, allied to the control of the flow, opens the possibility of obtaining and controlling the information and, from that, obtaining a greater structural power (Clement 2014; Segal 2017). The upstream collection method consists of focusing "directly on the cables and networks that pass through the United States, collecting data from American and foreign citizens to filter them under criteria determined by the agency" (Segal 2017, 13). The collection was done through two methods; direct cooperation with telecommunications companies, which forwarded the intercepted material to the intelligence agencies, and unilateral interception carried out by the agency (Clement 2014). Through these methods, the US government used the strategic positioning of the Internet's transport network to collect data and metadata from communications between citizens, companies, and even high-ranking authorities in other nations. (Clement 2014; Segal 2017)

To address these intractable realities, the authors propose to study cyberspace and cyber power based on specified fields. The location of power, for example, could be in combat actions (e.g., cyber-attacks), infrastructure arrangements, institutional relationships, or production/modulation of the discourse that drives the development of these technologies. Also, as posted by Betz and Stevens (2011) regarding cyberspace power, the complexity can be viewed and analyzed by methods of complex systems. In the database of each complex system, there is a web that codifies the interactions among the system's components (Barabási 2002).

Data and Methodology

Data

The database used for this work was the TeleGeography Global Internet Geography, a report produced by PriMetrica. The base gathers the transmission capacity of submarine cables from country to country, in MB/s, from the years

2011 and 2017. The base consists of data aggregated by PriMetrica from various sources, including governments and companies.

Important to note that the transmission capacity does not represent the flow (the actual used capacity) but the data of full transmission potential that each route has, see Table 1. The route is the connection between two countries (a dyad, for example, a connection between the United States with Brazil in 2011, a connection of the United States with China in 2011) by year. Countries that have two or more submarine cables connecting to other countries have the capacity of their cables calculated by the total capacity. The period in which the capacity is measured refers to the month of June of each year, and the historical series covers the period from June/2011 and June/2017.

The methods calculation employed 74 countries, but only the United States, BRICS countries, and the top five European countries, that best performed in the analysis, were fully investigated, resulting in 10 countries tracking their evolution through time. The focus of the analysis is to verify whether there was a fall in the hegemony and influence of the United States in the submarine cable network, and also whether the five best-ranked European and the BRICS countries increased their cyber power during the period. The parameters to be used as quantitative measures are the measures of centrality, described in detail in the next section, to rank the countries in power capacity and verify in what position they are, comparing the data in the years 2011 and 2017. We used this period in order to compare the results with those from Winseck (2017). In this sense, it is important to reinforce that our results may not reflect the current state of the art of these power dynamics. Future studies using the Social Network Analysis (SNA) method and more recent data can bring more insights into the current context.

Table 1. Variable description

Variable	Year	Definitions	Number of Countries	Observations	Source
International Internet bandwidth (Mbps)	2011	Country-by-Country international internet capacity in Mbps	74	848	Teleogeography
International Internet bandwidth (Mbps)	2017	Country-by-Country international internet capacity in Mbps	74	969	Teleogeography

Source: TeleoGeography — Global Internet Geography — https://www2.telegeography.com/

Methodology

Considering the theoretical bases of power pointed out by Winseck (2017) and Strange (1975), we employ submarine cables as the object of study to investigate the distribution of cybernetic power between countries. These critical infrastructures are interpreted as potential surveillance tools, with the main example of upstream collection, which considers the strategic positioning of each country within the network of overseas cables as a symbol of potential cybernetic power. It is important also to frame that this capacity depends on technological and legal conditions that not all the countries on the database have. Thus, given that submarine cables still have a high degree of complexity to be analyzed, we employ the Social Network Analysis (SNA) method to address the complexity.

The SNA methodology derives from the field of mathematics called the Study of Graphs. A graph represents two or more objects connected. The terms used in this field of study to name actors or objects are nodes; also referred to as points, and the connections between these nodes are called edges (Scott and Carrington 2011).

According to Scott and Carrington (2011), a graph representation allows indicating some valences that nodes and edges have. One of these properties is to assign a weight to the links, which can be a positive or negative value that can indicate, for example, the quality of the connection of these nodes, such as the intensity of the link or the distance between nodes. The term network is commonly used when valences such as these are applied (direction, weight, labels for nodes, etc.), thus illustrating the objective complexity that relationships can acquire when studying a social phenomenon. The SNA tool is derived from this, therefore studying systems of social relations represented by networks. A metric obtained through an SNA is the so-called centralities, which measure the prestige, power, and importance that a node has in a network. Among the possible centralities calculated, three are highlighted in this work; Proximity Centrality, Betweenness Centrality, and Eigenvector Centrality.

Proximity Centrality has as the main parameter the distance of a node from the others in the network. It is the distance between points of a network measured by the number of nodes necessary to travel from one point to another. In other words, the greater the proximity centrality of a node, the closer this node is to the rest of the points in the network. To obtain this number, the Proximity Centrality (Ci) of node *i* is calculated by adding the shortest paths

(geodesic distance) between node *i* and all other nodes in the network *(n–1)*. In this case, the result is inversely proportional to the magnitude of centrality since the smallest product represents the greatest centrality. The result is divided by *(n–1)* to normalize this formula to values between 0 and 1, thus transforming the highest score into the highest proximity centrality.

Betweenness Centrality seeks to illustrate how many occasions a node appears in the totality of all geodesic distances between nodes in a network. In other words, it reveals how many times a node bridges the shortest paths between all nodes in the network. The network centrality score is calculated by the fraction of the number of times a node appears in the geodesic distances divided by the totality of the shortest possible paths. The higher the proportion, the greater the betweenness centrality of a node.

The Eigenvector Centrality evaluates the influence that a point has on the informational path of a network. The Eigenvector Centrality of a node is proportional to the sum of the importance of its neighbors. This importance is attributed to the number of connections and Betweenness Centralities. It is calculated by assigning an eigenvalue of these parameters to all nodes in the network. It is then defined that nodes with links with high-scoring contribute positively to the score, while nodes with low-scoring nodes are penalized. After a certain number of iterations, that is, of assignments of these eigenvalues and recalculations from them, values of Eigenvector Centrality are assigned.

Inspired by Ruiz and Barnett (2015), we consider that the submarine cables corresponding to the Internet backbone are the network links in which the nodes are the nations through which these cables pass. According to the authors, when viewing the mesh of these cables as a network, the potential flow of data between each node is attributed as a parameter for determining the centralities of each node. Thus, they define the hierarchy of importance of each nation for the Internet infrastructure, considering the centrality of each country as the sum of the number of companies' centralities obtained. Thus, different from this study their nodes are companies, not countries.

Adapting the result to the submarine cable context, Proximity Centrality reveals which nodes are best positioned to influence the network as a whole. For example, communication that starts from a point with high centrality of proximity will reach the entire network faster than points with less centrality. In this sense, the higher the proximity centrality, the better the information broadcaster of the node is. The nodes that most influence the flow and dynamics

of communications are the best placed in betweenness centrality since they are the most common crossing points when considering the most efficient paths. Nodes with greater betweenness centrality are more important as gatekeepers of network communications. Lastly, eigenvector centrality assesses the influence and position of the node by scoring whether or not the connections close to it have relevant proximity and betweenness centralities. The measure is considered an overall influence score on the network, balancing the role of the broadcaster and gatekeeper (Ruiz and Barnett 2015; Scott and Carrington 2011).

Finally, it is essential to mention that our application rests on two premises. First, the analysis considers that all countries have the same capabilities for interception, data analysis tools, and programs to exercise their cyber power. This extrapolation is necessary to level the potential power of countries and analyze them from this perspective. The second premise relates to the fact that the ownership and maintenance of these cables are mainly shared by companies, which may or may not acquire a cooperative posture with the governments over which they are under jurisdiction. In this sense, it is considered that all cables connected to any country are subject to the sharing of information that passes through it, regardless of who owns the cable in question.

These premises present points of attention and limitations that the work offers. However, even though the analysis carried out here has these mishaps, it provides a general parameter on the distribution of power and the limits of potential territoriality.

Results and discussion

Proximity Centrality

Table 2 shows the results for the proximity centrality, where the ten countries selected are displayed with their ordinated initial (column 2) and final (column 5) positions and relative (column 3) and absolute (column 4) positions. Arrows upward indicate an increase in the centrality and downward a decrease. The following tables share the same pattern.

Table 2. Countries' positions on the Proximity Centrality

Country	Initial Position (2011)	Relative Position (2011 → 2017)	Absolute Position (2011 → 2017)	Final Position (2017)
Germany	2	↑	↑	1
United Kingdom	3	↑	↑	2
Netherlands	4	↑	↑	3
United States	1	↓	↓	4
France	6	↑	↑	5
China	5	↓	↓	7
Russia	15	↑	↑	10
India	8	↓	↓	12
South Africa	21	↓	↑	25
Brazil	59	↑	↑	26

Source: Authors using data from TeleoGeography — Global Internet Geography.

When analyzing the period's results, it is observed that the United States decreased in its relative and absolute power, changing from first place to fourth, losing importance to Germany, the United Kingdom, and the Netherlands, respectively, in the first, second, and third places. China remains the first representative of the BRICS in relative power in both periods, losing. However, one position compared to 2011, being seventh. At the end of the series, Russia appears in tenth and India in twelfth, gaining positions compared to 2011. South Africa in the twenty-sixth and Brazil in the twenty-seventh complete the list of BRICS, with the former losing four positions at the beginning of the series and the latter gaining twenty-three positions.

With these data, we can conclude how broadcaster power varied between these countries in the analyzed period. The first is that the United States has lost its position as the main strategic transmitter. This place is at the end of the series belonging to European countries such as Germany, the United Kingdom, and the Netherlands. When we analyzed the BRICS, two of the five countries in the bloc, Russia and Brazil, increased their relative and absolute influence as network broadcasters. China and India lost relative and absolute influence, while South Africa lost relative influence, but improved its absolute score.

Betweenness Centrality

Considering the centrality of Betweenness, Table 3, the United States started the series in 2011 placed as the leader. Germany appears in second place, followed by the United Kingdom, the Netherlands, and France. China emerges as the first representative of the BRICS block, in sixth place, followed by South Africa and Russia in seventh and eighth position. India is fourteenth, with Brazil closing the BRICS block in the thirty-sixth.

Table 3. Countries' positions on the Betweenness Centrality

Country	Initial Position (2011)	Relative Position (2011 → 2017)	Absolute Position (2011 → 2017)	Final Position (2017)
United States	1	-	↓	1
Germany	2	-	↓	2
United Kingdom	3	-	↑	3
Netherlands	4	-	↑	4
France	5	-	↑	5
Russia	8	↑	↑	6
South Africa	7	-	↑	7
Brazil	36	↑	↑	8
China	6	↓	↓	10
India	14	↓	↓	19

Source: Authors using data from TeleoGeography — Global Internet Geography.

When analyzing the end of the series, the United States remains the leader, but with a lower score than the initial series. Germany, the United Kingdom, the Netherlands, and France occupy the same position in 2017 as in 2011. In sixth place, Russia appears as the first representative of the BRICS bloc, followed by South Africa and Brazil in the seventh and eighth position, respectively. China occupies the tenth place, while India appears in the nineteenth, closing the list of these countries.

Comparing the beginning and the end of the period, we observe that the United States remained the main gatekeeper among the countries analyzed. However, its influence has been reduced, as indicated by the lowest score in 2017. European countries maintained their position in relative terms, but Germany declined its

power in absolute terms, while the United Kingdom, Netherlands, and France increased its importance as a bridge. Looking at the BRICS, Russia, South Africa, and Brazil increased their influence between 2011 and 2017 in absolute terms. China and India, however, lost their influence in absolute and relative terms, presenting lower scores and dropping their position in the ranking.

Thus, the results of the Betweenness Centrality indicate that, although the United States remained in the leadership of the ranking as the most influential gatekeeper, there was a loss of the country's score in this aspect. Meanwhile, except for Germany, there was again influential in the scores of other European countries (the United Kingdom, Netherlands, and France), which maintained the same position in the ranking.

Eigenvector Centrality

Table 4 shows that at the beginning of the series, the results of Auto-Vector Centrality, the United Kingdom is in the lead, followed by the United States. Then, Germany, China, the Netherlands, and France are positioned as the top five. Looking at the rest of the BRICS block, India appears in eighth, followed by Russia in the nineteenth, South Africa in twenty-second, and Brazil in seventy-second.

Table 4. Countries' positions on the Eigenvector Centrality

Country	Initial Position (2011)	Relative Position (2011 → 2017)	Absolute Position (2011 → 2017)	Final Position (2017)
United Kingdom	1	-	-	1
Germany	3	↑	↑	2
Netherlands	5	↑	↑	3
France	6	↑	↑	4
United States	2	↓	↓	5
China	4	↓	↓	7
India	8	↓	↓	11
Russia	19	↑	↑	13
South Africa	22	-	↑	22
Brazil	62	↑	↑	42

Source: Authors using data from TeleoGeography — Global Internet Geography.

At the end of the series, the United Kingdom remained in the first position. The United States and China lost relative and absolute influence to Germany, France, and the Netherlands, which increased their rankings and scores. The remaining BRICS countries, except India, have lost ranking positions and points — South Africa, Brazil, and Russia — but increased their scores, with the former maintaining its position and the latter two moving up in the rankings.

Discussion

Measuring cyber power by the control of submarine cables capacity, the main finding is that the United States lost its hegemony in controlling the Internet infrastructure between 2011 and 2017. Part of this loss is greatly due to the increased power of the European countries, especially Germany, the Netherlands, and the United Kingdom. Also notable is the power rise of the BRICS countries, led mainly by China, but also counting on the advance in the strategic positioning of infrastructure control mainly by Russia and Brazil and the maintenance of the influence of players already relevant at the beginning of the series, such as India and South Africa.

The results corroborate the main findings of Winseck (2017): namely, the United States' power and control over international Internet resources at the infrastructural level and in terms of Internet traffic has declined over time, while some European and BRICS countries have seen a corresponding increase over time. In Europe, Germany, the United Kingdom, the Netherlands, and France stood out in terms of the relative increase in their control over Internet infrastructure resources and capacity. In the BRICS group, Brazil and Russia gained the most power. Surprisingly, while China has maintained its leadership among the BRICS countries, in relative terms, it has lost power based on the measures we assess in this paper.

Specifically, the results show that the central hub of countries with broadcaster characteristics changed from the United States to Europe. This can be read from the change in position in the Proximity Centrality ranking, initially led by the United States, in 2011, and surpassed by Germany, the Netherlands, and the United Kingdom in 2017. The evolution of the European countries can be measured not only in their positioning but also by the score of the Proximity Centrality criterion, which increased in the mentioned countries while it decreased in the United States. Regarding BRICS countries, it appears that China, the main player in the block

and India, followed the same trend as the United States, decreasing its position and its overall score. However, Brazil and Russia climbed the rankings as their scores increased. South Africa showed an ambiguous move, increasing its score.

Betweenness Centrality reveals that the United States still maintains leadership in this aspect, losing the overall score and narrowing its distance to Germany, the United Kingdom, and the Netherlands. These last two kept the same position at the beginning of the series but with a higher overall score. While maintaining its position, Germany also lost points in the absolute category. In this way, even though it has remained the main gatekeeper of the analyzed network, the United States lost a margin of influence over these European countries at the end of the series compared to the beginning. In the BRICS bloc, China loses its role as the main gatekeeper, overtaking Russia, South Africa, and Brazil, which increased their positions and scores. Like China, India also loses ranks and absolute scores compared to the beginning of the series.

Finally, analyzing the Eigenvector Centrality measure, the United Kingdom remains from the beginning to the end of the series as the country with the greatest balance between the two centralities calculated. It can be said that it had the best strategic positioning among the countries analyzed in the period. The United States, which started the series in second place, drops to the fifth position, again demonstrating the loss of its hegemony of power on the Internet. From the second to the fourth places finish the series being occupied by Germany, Netherlands, and France, respectively, forming the best-positioned countries with European countries. For the BRICS countries, China remained the great leading country; however, losing influence and position during the period, as did India. Brazil and Russia, however, rose in rank and increased their influence, even though their relative position continuing not to place in the top 10.

The Social Network Analysis methodology points out the evolution of cyber power with a specific and contextualized form, analyzing data through the lens of a network. That allows us to see exactly which European countries represent the main challenges for the United States regarding internet hegemony; the major gainers of power and prestige when considering these metrics are Germany, the Netherlands, and the United Kingdom. Looking at the BRICS, China, even though it remains the main protagonist of the bloc, lost absolute power in all metrics, ruling out the possibility that it will become the new hegemonic actor controlling the Internet backbone. During the analyzed period, Brazil and Russia stand out as the foremost gainers of power and prestige.

Regarding the *structural power* framework brought by Lukes (1975) and Strange (1975), the results indicate deconcentration of the power among these main actors, according to the narrowing measured differences between scores results. This scenario can lead to an enhanced protagonism of some players, such as China and the European countries, and to the surging of new actors such as the remaining BRICS countries. Embedded into this process are growing tensions among these players, with some incomers moving towards the development of national cyber capabilities as well the contenders struggling to keep their dominance over other layers of the network.

An example given by Winseck (2017) relates to the Snowden disclosures of 2013. The author argues that the global surveillance program called Five Eyes led by the United States only could operate with the cooperation of other nations, especially the European ones, indicating a lack of hegemony in the infrastructure layer. Regarding the content layer, the restricted operation of some companies occurs in the sense of protecting the so-called cyber sovereignty. In China, for instance, most American technology companies such as Meta (Facebook) and Alphabet (Google) are prohibited from operating there with the allegation of their national security being protected. Similarly, the Chinese app TikTok suffered restrictions of use in 2019 and 2020 under the Trump administration. (Slaughter e McCormick 2021)

Another example that relates to these tensions caused by this decentralization of structural power is the dispute over the 5G standard dominance rolled by the United States and China. The episode is described in the literature by the combative posture of the US government initiated against the implementation of 5G technology by the Chinese company Huawei, both in its territorial domains and those of allies. (Hoffmann, Bradshaw and Taylor 2020; Inkster 2019; Kaska Beckvard and Minárik 2019; Shoebridge 2018). The company stands out for being identified as one of the only companies in the current context that can feasibly produce, in scale and cost, the components of a 5G network. (Inkster 2019; Kaska, Beckvard and Minárik 2019). With this innovation, technologies considered of great impact are made possible, such as the development of interconnected robotics and artificial intelligence, allowing them to be applied at a global scale with a viable cost. The literature points out that the actor who dominates the next technological evolution of the infrastructure will have the components of the next industrial revolution and increase enormously its comparative advantages in relation to rivals, both from an economic and military point of view.

Regarding the contenders, one example is the 5G dispute. The central argument for the United States to stop Huawei was that the 5G infrastructure would be a means of the Chinese government to spy the populations of the United States and allies — such as Australia, Japan, New Zealand, Germany and the United Kingdom — by controlling the information flows. The direct consequence of this combative stance was the introduction of measures prohibiting the company from acting in the composition of the telecommunications infrastructure within the territory of the United States and the aforementioned allies (Kaska, Beckvard and Minárik 2019).

Supported by the results obtained and the examples cited, a possible conclusion is that those tensions tend to increase in the next years, which indicates the setting of cyberspace as an important matter in national and international security agenda. In this sense, methodologies that offer an objective measurement of power, such as the one presented in this study, can contribute both to the academic exercises and as auxiliary tools to orient policies to issues in international affairs.

Finally, it is important to observe that this study has two important limitations. First, the measure of the potential power that we employed is based on the full capacity of information transmission and not actual traffic, given the limited information on Internet flows compared to the capacity of the submarine communication cables data. The second limitation is that this paper does not consider the ownership of the submarine cables, just the countries where the connections occur. However, based on the reduced available dataset on ownership, the results for countries are similar.

Final Remarks

We employ Social Network Analysis to deal with the high degree of complexity in the submarine cables' geography design and measure the potential cyber power of selected countries.

The main results reinforce the conclusions in Winseck (2017), especially regarding the loss of hegemony of Internet control by the United States to countries of the European block and the BRICS between 2011-2017. But they go further by pointing out specifically which countries performed better in the network context.

It is observed that the main challenge to hegemony was the main European countries, led mainly by Germany, the United Kingdom, and the Netherlands,

which in the three metrics used in this study, narrowed the margin or surpassed the United States in the centrality scores. Although it remains one of the main protagonists in all aspects, this indicates that the US no longer occupies a hegemonic position in these areas. The conclusion is that all the countries of the European block increased their power as broadcasters, gatekeepers, and influence in general on the network. At the same time, the United States declined in all these aspects.

The block of BRICS also gained, in general, a greater projection in the context of infrastructure control and strategic positioning of the submarine cable ecosystem. However, the performance of the block's countries was ambiguous. China remains the leading player in the block but loses positions and scores in all metrics during the series. The same occurred with India, which remained the second most influential country in the block regarding Proximity and Eigenvector. However, its score and positioning decreased during the series. On the other hand, Russia and Brazil showed progress in positioning and scoring in all centralities, standing out in the block as countries that acquired the most influence over the period analyzed. Finally, South Africa was the most ambiguous performer, increasing its score across all metrics, maintaining its Eigenvector and Betweenness centralities, but decreasing some positions in the Proximity Centrality. The conclusion is that the main players at the beginning of the series, China and India, had their importance reduced in the network as a whole. Still, they remained the main protagonists of the bloc, even with the positive performances of Russia, Brazil, and South Africa.

From these conclusions, it is observed that the Social Network methodology reaches similar overall findings to other analysis methodologies, such as the one used by Winseck (2017). In addition, it allows more details regarding the relative positions of each agent involved in the dispute. Furthermore, it contributes to the field by presenting an application of this methodology in a network context, such as analyzed here, offering an objective measurement of cyber power. The same method can potentially explore other layers of cyberspace, especially those organized in network models.

Results and examples illustrate that cyberspace increasingly becomes an important field of dispute among states and corporations. That regards economic and national security issues, setting itself a relevant topic to the International Relations academy. However, it should be noted that since the main subject of the paper is to compare methodologies, the results obtained must be read according

to the time of data, thus valid for 2011-2017. In this sense, future studies must use current data on submarine cables applied to Social Network Analysis to describe the current dynamic.

References

Arquilla, John, e David Ronfeldt. 1993. "Cyberwar is coming!" *Comparative Strategy* 12 (2): 141–65.

Barabási, Albert-László. 2002. *Linked the New Science of Networks*.

Betz, David J., e Tim Stevens. 2011. "Chapter One: Power and Cyberspace". *Adelphi Series* 51 (424): 35–54. https://doi.org/10.1080/19445571.2011.636954.

Choucri, Nazli, e David D. Clark. 2018. *International Relations in the Cyber Age: The Co-Evolution Dilemma*. Cambridge, MA: The MIT Press.

Clement, Andrew. 2014. "NSA Surveillance: Exploring the Geographies of Internet Interception". Em *IConference 2014 Proceedings*. iSchools. https://doi.org/10.9776/14119.

Costigan, Dean S, Michael A Hennessy, North Atlantic Treaty Organization, Partnership for Peace, e Consortium of Defense Academies and Security Studies Institutes. 2016. *Cybersecurity: A Generic Reference Curriculum*. Norfolk, VA; Kingston, ON; Garmisch, Germany: NATO ; National Defence ; PfPC of Defense Academies.

Freeman, Linton C. 1978. "Centrality in social networks conceptual clarification". *Social networks* 1 (3): 215–39.

Hoffmann, Stacie, Samantha Bradshaw, e Emily Taylor. 2020. "Networks and Geopolitics: How Great Power Rivalries Infected 5G", 37.

Inkster, Nigel. 2019. "The Huawei Affair and China's Technology Ambitions". *Survival* 61 (1): 105–11. https://doi.org/10.1080/00396338.2019.1568041.

Kaska, Kadri, Henrik Beckvard, e Tomáš Minárik. 2019. "Huawei, 5G and China as a Security Threat". *NATO Cooperative Cyber Defence Centre of Excellence*, 26.

Kuehl, Daniel T. 2009. "From Cyberspace to Cyberpower": Em *Cyberpower and National Security*, editado por Franklin D. Kramer, Stuart H. Starr, e Larry K. Wentz, 24–42. University of Nebraska Press. https://doi.org/10.2307/j.ctt1djmhj1.7.

Kurbalija, Jovan. 2017. "Uma introdução à Governança da Internet", 246.

Libicki, Martin C. 2012. "Cyberspace is not a warfighting domain". *Isjlp* 8: 321.

May, Christopher. 1996. "Strange Fruit: Susan Strange's Theory of Structural Power in the International Political Economy". *Global Society* 10 (2): 167–89. https://doi.org/10.1080/13600829608443105.

Ruiz, Jeanette B., e George A. Barnett. 2015. "Who Owns the International Internet Networks?" *The Journal of International Communication* 21 (1): 38–57. https://doi.org/10.1080/13216597.2014.976583.

Scott, John, e Peter J. Carrington, orgs. 2011. *The SAGE Handbook of Social Network Analysis*. London ; Thousand Oaks, Calif: SAGE.

Segal, Adam. 2017. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. Unabridged Audio edition. Gildan Audio and Blackstone Audio.

Shoebridge, Michael. 2018. "Chinese Cyber Espionage and the National Security Risks Huawei Poses to 5G Networks". *Macdonald-Laurier Institute*, Commentary,.

Slaughter, Matthew J., e David H. McCormick. 2021. "Data Is Power", 16 de abril de 2021. https://www.foreignaffairs.com/articles/united-states/2021-04-16/data-power-new-rules-digital-age.

Strange, Susan. 1975. "What Is Economic Power, and Who Has It?" *International Journal* 30 (2): 207–24. https://doi.org/10.1177/002070207503000202.

Tirtea, Rodica. 2017. "ENISA Overview of Cybersecurity and Related Terminology", 8.

USA, DoD. 2021. "DOD Dictionary of Military and Associated Terms". https://irp.fas.org/doddir/dod/dictionary.pdf.

Ventre, Daniel. 2012. *Information Warfare*. John Wiley & Sons.

Winseck. 2017. "The Geopolitical Economy of the Global Internet Infrastructure". *Journal of Information Policy* 7: 228. https://doi.org/10.5325/jinfopoli.7.2017.0228.