The Tor Network and Non-State Actors

An Analysis of the Diffusion of Power in Three Dimensions

Barbara I. S. Calderon

2018

Contents

List of Figures

List of Tables

Abstract

The diffusion of power was a phenomenon first described by Susan Strange in the context of International Political Economy (IPE) in 1996. The phenomenon encompasses the concepts of relational and structural power, which are essential for understanding the IPE discipline. Although described in the 1990s, the diffusion of power did not address the cyber domain, nor explicitly the technological revolutions that culminated in the global computer network. In cyberspace, various actors operate to impose their authority over individuals and services. In this context, at the beginning of the 21st century, the low-latency anonymous network known as "The Onion Router" emerged, being part of the so-called "Dark Web" — a region of cyberspace characterized by active efforts to shield communication, privacy, and specific users. This research aims, through journalistic articles published between 2007 and 2017, to analyze the diffusion of power in the TOR network across three dimensions: authority, control, and results.

Keywords: Diffusion of Power. Dark Web. TOR Network. Structural Power. Relational Power. International Political Economy.

Chapter 1

Introduction

The present research falls within an area of study still uncommon within the field of International Relations (IR): one that treats the cyber domain as the new stage for actions among various actors in the International System (IS). This area is part of a broader thematic umbrella that discusses the role of Science and Technology (S&T) within the discipline and seeks to understand their influence on international affairs.

Authors have expressed the importance of S&T for the various dynamics addressed by the discipline of IR (SKOLNIKOFF, 1993; WEISS, 2005; KRIGE; BARTH, 2006; MATTHEWS, 1997). Some emphasize that S&T is a powerful and persistent factor, capable of producing social changes and thus culminating in international affairs (SKOLNIKOFF, 1993; MATTHEWS, 1997)[1]. Others point out that this relationship also has an inverse meaning—that is, when S&T themselves are influenced by international affairs, either directly or indirectly (WEISS, 2005, p.297)[2]. That is, just as international affairs are influenced by technological development, the reverse would also be true.

[1]Indeed, according to Skolnikoff (1993), after the advent of World War II and the discovery of a myriad of scientific breakthroughs—including the discovery of nuclear fission by the U.S. Manhattan Project—any doubt about the relevance of technology for the purposes of the State was extinguished. In this era, almost all the technology that the world may assimilate or deal with is the result of a calculated production of decisions made within existing political processes. In fact, the author himself questions which aspects, if any, of international affairs have not yet been "touched" by S&T. In particular, Skolnikoff (1993) points to evidence of the evolution of S&T in international affairs: the massive deployment of strategic nuclear forces; the Chernobyl nuclear accident; the monetary transactions occurring abroad through digital financial markets—which, at the time, already surpassed 500 billion U.S. dollars daily; and the near-total eradication of smallpox. Another author, Jessica T. Matthews (1997), in the mid-1990s, pointed out the relative decline of States in the face of the rise of non-state actors on the global stage. These actors were to be "catapulted" onto the global stage due to the telecommunications and computer revolution—the political and social consequences of which, according to her, had until then been virtually ignored by academia.

[2]Weiss (2005) points out that the direct effects can be felt in four ways: first, public opinion directly affects public support for investments in S&T; second, the goals of foreign policy have the capacity to alter national priorities, reallocating certain investments to the detriment of others; third, the state of relations between two countries affects the migration of scientists, their communications, collaborations, access to study objects, etc.; fourth, international agreements affect the global strength directed toward the protection of intellectual property. Indirect effects operate through mechanisms of Economics, Law, Politics, and Culture.

Despite the relevance of the topic for IR, the academic literature on it remains limited. In this regard, Eugene Skolnikoff stands out as one of the major figures in the convergence between S&T and IR. His work *The Elusive Transformation: Science, Technology and the Evolution of International Politics* (1993) became a reference point regarding the consequences of scientific and technological changes on the evolution of international politics in various dimensions. In this work, Skolnikoff (1993) also reflects on the reasons why the topic of S&T has been neglected by scholars in IR. He suggests, for instance, that information and knowledge arising from S&T are not treated with the importance they deserve because the perception, on the part of IR scholars, is that they are sometimes "obscure" topics. This obscurity is the reason they are relegated to the second or even third plan.[3]. Author Weiss (2005) complements this view of difficulty in assimilation: according to him, the topic of S&T, when addressed by the field of IR, is approached without a defined logical structure. It is as if the subject were composed, apparently, of residual topics from other themes on the IR agenda.

In the 1990s, the revolution of information systems, as an aspect within S&T, was a relevant point of academic discussion. Regarding authors who reflected on the interface between the theme and IR, four scholars stand out: Strange (1988), Skolnikoff (1993), Builder (1993), and Nye (2011). In common, these authors indirectly pointed out how technological changes can impact State power.

In 1988, before the commercialization of the Internet, the British scholar Susan Strange published *States and Markets*—considered a starting point for understanding structural power and, for this reason, a major milestone in the literature of IR and International Political Economy (IPE). In this work, while discussing the *knowledge structure*, Strange (1988) reflected on the technological revolution emerging at the end of the 20th century. In particular, three considerations stand out: (1) the development of sophisticated computer systems with accessibility (availability and low cost) to the masses; (2) the expansion of communication systems using satellites orbiting the planet; (3) and the aspect of language digitization, which significantly reduces the linguistic barriers separating human groups. In general, Strange (1988) outlined insights into the technological revolution and its implications for the provision and control of information and communication systems. She also highlighted changes in the use of language and non-verbal communication channels; in perceptions she deemed fundamental to the human conditions that influence judgments and, through them, political and economic policies and decisions. These points are essential for understanding the dynamics of the knowledge structure, the diffusion of power, and the impact of these elements on State power.

Another scholar, Eugene Skolnikoff, in 1993—during the threshold period of the com-

[3]Skolnikoff comments on this when he states that "even scholars concerned with theoretical issues in international relations tend to treat science and technology as static 'givens', or as emanating from impenetrable black boxes." (SKOLNIKOFF, 1993, p.9)

mercial and global opening of the worldwide computer network—did not fail to ponder information technologies. Although he did not explicitly address the Internet and its implications for international politics, he discussed the relevance of recent technological changes to political power. According to him, the introduction of information technologies would considerably increase the limitations on the centralization of political power.[4] For Skolnikoff (1993), this conclusion is so widely accepted among commentators on international politics that analyses of international affairs, to a large extent, refer to information technologies as key factors that would undoubtedly bring about changes in the international system. (SKOLNIKOFF, 1993). However, he makes it clear that this will not result in the dissolution of the state or a reduction in its relevance in the international system.

At the threshold of the commercial opening of the Internet, Carl H. Builder was another author who contributed to the analysis of the impact of the information systems revolution on international relations. According to Builder (1993), part of the enthusiasm about the new information age stems from the possibilities that the exploitation of hardware offers in relation to power. This era, responsible for shortening the distances across the globe, disseminated a new perspective on power based on information. For Builder (1993), the state faces a dilemma: should it allow or deny free communication through the new information systems? Permitting it would result in granting the power of information to individuals. And, in possession of this power, they would have sufficient capacity to challenge various hierarchies that were themselves established and maintained through the logic of control and denial of information. On the other hand, denying access to communication and the technologies arising from this new information age could mean missing the opportunity to firmly integrate into the global economy.[5]

Finally, in 2011, the renowned IR scholar Joseph Nye Jr. published the work *The Future of Power*, in which he discussed the relevance of the new information age for rethinking power. In this work, Nye reflects on the technological revolutions of the late 20th century and how they gave rise to a new form of power, which he termed "Cyberpower." It

[4]Especially regarding these limitations, he states that "The effects are easier to see and analyze in those nations, for authoritarian governments, aware of the importance of information to their maintenance of power, have made more conscious attempts to control information flow. But, for all governments, information technologies have similar implications for autonomy, openness, and decentralization of power." (SKOLNIKOFF, 1993, p. 102).

[5]Builder (1993) also addresses other relevant points on the topic. One of his questions revolves around the apparent "revolution" of information at the end of the 20th century: is the world facing a transition or a revolution? If it were a transition, it would be a shift from a society with relative information poverty to one with relative information abundance. As such, this transition would have revolutionary effects on all existing institutions and hierarchies. However, if the world is facing a revolution, the most obvious victims of this dynamic are nation-states and their governments. This does not mean they would disappear, but they would give way to new actors. Thus, an important consequence of this new information age is the emergence of transnational factions. Similar to Strange (1996), Builder (1993) also discusses the power concentrated in the nation-state and its subsequent diffusion to new non-state actors.

is in this hybrid regime scenario—where the concrete reality of cables, machines, computers, satellites, and other infrastructure merges with the virtual abstraction of digital bytes and interactions among agents—that the fabric of the new domain of the 21st century is woven: the cyberspace. In this realm, the state and new actors emerge to seek space and compete for power. (NYE, 2014). However, he advises caution when considering power in this domain, as cyberspace will not replace geographical space nor extinguish state sovereignty. (NYE, 2010).

In summary, the aforementioned authors, despite making relevant considerations about the ongoing technological changes at the end of the 20th century and their impact on state power, were cautious in asserting that such changes do not signify a reduction in the relevance of the state in the international system (IS), nor its extinction.

Before the commercialization and mass use of the Internet, if there was already discussion about the need to include the topic of Science and Technology (S&T) in the range of issues relevant to the field of International Relations (IR), today this need is paramount.[6] There is a need for part of the research efforts to focus on the intersection between Information Systems, Science and Technology, and International Relations—considering the development of the topic and its significant public interest, especially in the range of issues focused on cyberspace. The latter, in fact, has instilled political and economic implications significant enough to reverberate in research across different fields of study that intersect with themes on the IR agenda.

When it comes to research and investigations in the field of IR and cyberspace, the topics vary widely. Some research focuses on the technological dimension of the Westphalian system in the Internet age (BRUNN, 1998; MILLS, 2012; TIKK-RINGAS, 2012; DEIBERT, 2013; DEMCHAK; DOMBROWSKI, 2013). Other studies seek to understand IR through the distinctive lens of Information Technologies (IT)—whether analyzing the convergence of the "digital age" and the "age of terror" (DERIAN, 2003); or examining the role of the state, private actors, and online commerce in regulating information flows (FARRELL, 2006). Much has also been discussed about digital governance—with particular emphasis on the investigations by Canabarro (2014). Other researchers advocate for a view of IR within the cyber domain to investigate digital governance (VAISHNAV; CHOUCRI, 2013; MUELLER; SCHMIDT, 2013). Additionally, there are those who discuss the role of the worldwide web in diplomatic and foreign policy issues (ROSS, 2011). After all, since politics is an action linked to the activities of actors in a collective context, much has been pondered about the political activities of these actors in the cyber domain (CASTELLS; CARDOSO, 2005; ROCHE; BLAINE, 2014; SIEDLER, 2016). Above all, perhaps the most investigated topics are two: cybersecurity (NISSENBAUM, 2005; NYE, 2011; CHOUCRI; GOLDSMITH, 2012; KALLBERG; THURAISINGHAM, 2012;

[6]Eugene Skolnikoff (1993) is perhaps the leading figure in this agenda that advocates for the inclusion of technology in the issues of the discipline of International Relations.

KRAMER, 2012; HATHAWAY, 2012; CEPIK; CANABARRO; BORNE, 2014) and cyber warfare (BERENGER, 2006; WALSH; BARBARA, 2006; MICHALSKI; GOW, 2007; CLARKE, 2009; LIBICKI, 2009; CORNISH et al., 2010; LAWSON, 2012; HURWITZ, 2013; JUNIO, 2013; CEPIK; CANABARRO; BORNE, 2015; JAJODIA et al., 2015; SCHREIER, 2015; SCHNEIDER, 2016). There is, above all, a significant gap in the study of the Dark Web and IR, this thesis' topics.[7]

This research is concerned with the structure of knowledge in the context of the cyber domain. Specifically, it seeks to investigate evidence of the diffusion of power through the low-latency anonymous network *The Onion Router* (TOR)—a component of the Dark Web. The latter is a peculiar part of the global computer network, with its own definition. Therefore, we adopt the field of International Political Economy (IPE), from the perspective of Strange (1988, 1996), as the theoretical framework for this study, as we believe this approach has sufficiently relevant elements to explain the phenomenon of the diffusion of power in the cyber domain, encompassing both the plurality of actors and the digital context in which they operate.

1.1 Delimitation of the Theme and Research Question

In her 1996 work, *The Retreat of the State: The Diffusion of Power in the World Economy*, Susan Strange explicitly states that structural power can be observed through an analytical framework that defines "who-gets-what" in global society based on four basic structures: the security structure, the production structure, the financial structure, and the knowledge structure.[8] In summary, the objective of her work is to draw attention to the power that originates from these structures, particularly from non-state actors. Due to this power, such actors have the capacity to alter outcomes in the International System. Structural power, as defined by Strange (1988), is derived from and conditioned by these four structures.

[7]The SCOPUS database—the largest database of abstracts and citations of peer-reviewed literature, according to its own definition—when the user conducts a search using the keyword "dark web," restricting the fields to "social sciences," "decision sciences," "business, management and accounting," "economics, econometrics and finance," "multidisciplinary," and "arts and humanities," that is, areas related to IR, the search returns 38 results. When, instead of "dark web," the keyword "tor network" is used, the result is 24 occurrences. In other words, the total is 62 documents. When restricting the fields to "computer science," "engineering," and "mathematics," using the keyword "dark web," there are 87 results. The keyword "tor network" provides 165 documents. In total, there are 252 documents—more than four times the results in the social sciences fields.

[8]Within each of these structures, power over others—and also over the mix of values within the system itself—is exercised within and beyond the borders of nation-states by: (1) those who are in a position to threaten or provide security; (2) those who are in a position to refuse or provide credit; (3) those who define what is produced, where, by whom, and under what conditions and terms; (4) those who control access to knowledge and information, as well as those who are in a position to define the nature of knowledge (STRANGE, 1996).

Through this analytical framework on the nature of power, the author managed to distance herself from the traditional currents of the IR discipline that upheld the position of the nation-state as the main actor in the International System—and, according to her, often the only one.[9] Strange (1996), in turn, seeks to argue for the existence and relevance of other actors beyond the State in global politics and economy: international organizations, transnational corporations, transnational professions, multinational companies, etc.

The focus of our research is the analysis of the diffusion of power in the context of the anonymous TOR network, embedded within the cyber domain. Due to the nature of this network, the diffusion of power is based on the fourth structure defined by Strange—the knowledge structure. Regarding power and this structure, Strange (1988) stated:

> *[The power derived from the knowledge structure is the one that has been most overlooked and underrated. It [...] comprehends what is believed (and the moral conclusions and principles derived from those beliefs); what is known and perceived as understood; and the channels by which beliefs, ideas and knowledge are communicated—including some people and excluding others. [...] Analysis of the knowledge structure is therefore far less advanced and has far more yawning gaps waiting to be filled, than analysis of other structures. [...] Ordinary people in their everyday wisdom have always recognized that 'knowledge is power'. But in a rapidly changing global knowledge structure such as we have today it is by no means clear to social scientists who has that power. One trouble is that the power derived from the knowledge structure is often very diffused. (STRANGE, 1988, p.119).].*

In the realm of cyberspace, which emerged at the end of the 20th century, it is possible to observe a multiplicity of actors using the Internet to carry out their activities. In this public Internet—free of restrictions and devoid of technologies that provide users and their communications with privacy and anonymity—concerns about surveillance by companies and government entities are voiced by activists and whistleblowers (LANDAU, 2013; SCHEUERMAN, 2014; BAKIR, 2015; WALSH, MILLER, 2015; MURATA, ADAMS, PALMA, 2017). For this reason, the low-latency TOR network—which seeks to provide privacy and anonymity to users and communications through the global Internet—enters the debate on surveillance and privacy in the digital age as an important communication channel. Through the Dark Web, specifically the TOR network, various actors have carried out political operations that have resonated in the media in recent times and have become known to the general public. To illustrate this point, we cite: the WikiLeaks group led by Julian Assange (WIKILEAKS, 2016); the hacktivist group Anonymous (COLLEMAN, 2011); the transnational organization Reporters Without Borders (REPORTERS WITHOUT BORDERS, 2016); former National Security

[9] In particular, Realism, in its various strands, views the nation-state as the holder of power in international relations—whether through the conception of relational power or material power.

Agency (NSA) agent Edward Snowden—who uses the TOR network, among other mechanisms, to safeguard his communications and ensure privacy (LEE, 2015); the terrorist group Al-Qaeda (COHEN-ALMAGOR, 2012); the Silk Road online drug marketplace (CHRISTIN, 2012); cryptocurrencies like Bitcoin, widely used in commercial transactions on the Dark Web's anonymous networks (KUHN, 2015); and, to a lesser extent, jihadist terrorists and pedophiles (MOORE; RID, 2016).

Since, according to Strange (1988), the structure of knowledge comprises the channels through which beliefs, ideas, and knowledge are communicated, it is reasonable to investigate the diffusion of power within the TOR network and the actors who operate power through this channel. Thus, the research question was formulated to understand how, and to what extent, the TOR network increases the diffusion of structural power in the 21st century. The aim of this research is to investigate the issue of the diffusion of power in this region of cyberspace, examining evidence of the increase or decrease of power by non-state agents. Such evidence should, above all, be tied to outcomes in the geographical real-world dimension of the international system (IS).

1.2 Justifications

There are six main justifications that underpin the choice of the theme and scope of this research: first, the rise of the "cyber" theme as a niche for study in International Relations (IR). Second, the urgency of the topic of anonymous networks in the debate on global digital surveillance perpetrated by governmental and corporate entities. Third, the choice of the structure of knowledge over other structures addressed by Strange (1988)—security, production, and finance—is justified. Fourth, the potential academic contributions of this research to the studies on the diffusion of power in the fields of International Political Economy (IPE) and International Relations (IR). Fifth, the choice of the low-latency anonymous network TOR, the selected journalistic media, and the actors presented in this research are also justified. Lastly, the author's personal motivations for the choices and boundaries set in this research.

First, the rise of the "cyber" theme occurred primarily from the new millennium onward. The end of the last century brought about paradigm shifts in technological, political, and social dimensions. According to Castells and Cardoso (2005), this century was responsible for "catapulting" human life into a new phase in technological terms. The period encompassing the significant changes related to the technological "leap" experienced by society is known in the literature as the "Information Age" or the "Network Society." The latter, by definition, "[It is] the social structure that results from the interaction between the new technological paradigm and the overall social organization" (Ibid., p.3). There is a novel element in this society, which is the "microelectronic foundation of network technology that provides new capabilities for an ancient form of social organization:

in networks" (Ibid., p.4). In other words, humans did use the communication networks prior to the 20th century, which were quite common, but the novelty arises from the nature of the network connections, which are now based on digital technology and have a truly global reach (Ibid., p.4).[10]

It is necessary to recognize that, at the end of the 20th century, a new domain emerged that was not adequately embraced by the field of International Relations (IR)—despite its global reach and social and economic character. However, even though it does not have the same volume of studies as the traditional areas of the discipline, considerable advances have been made, as previously highlighted in this research. One of the reasons why the "cyber" theme has gained more space within the scope of the social sciences—although still relatively smaller than in the natural sciences—was the publication, in June 2013, by the British newspaper *The Guardian*, of a series of reports that became known as the "Snowden Revelations," the content of which reverberated across various countries simultaneously. The detailed information provided by the newspaper came from secret documents leaked by Edward Snowden, an employee of Booz Allen Hamilton, a company providing services to the National Security Agency (NSA) of the United States of America (USA). According to Landau (2013), the documents revealed numerous surveillance and espionage schemes focused on the Internet.[11] From the Snowden Revelations, the academic community published several studies on the subject from different perspectives (Landau, 2013; Chadwick & Collister, 2014; Landau, 2014; Lucas, 2014; Scheuerman, 2014; Toxen, 2014; Bakir, 2015; Branum & Charteris-Black, 2015; Lyon, 2015; Merck, 2015; Nocetti, 2015; Qin, 2015; Salvo & Negro, 2015; Walsh & Miller, 2015; Gürses, Kundnani & Hoboken, 2016; Murata, Adams & Palma, 2017). Authors Castells and Cardoso (2005) state that the Network Society currently constitutes the core of contemporary societies. For this reason, it is imperative that new studies be conducted on the "cyber" theme.

Secondly, issues related to the maintenance of rights and civil liberties that can ensure privacy, consent, and free expression on the Internet gained new dimensions after the massive revelations of digital surveillance perpetrated by the U.S. through the In-

[10]Castells and Cardoso (2005) make a small caveat: although considered global, this network society is diffuse and presents an element of exclusion by not including the entirety of humanity.

[11]Landau (2013) outlines several of them: the domestic telecommunications metadata collection program of Verizon Business Networks Services—including the "who," "what," and "when" of telephone calls; the NSA's "PRISM" program, which targeted specific Internet communications and data storage of individuals outside the borders of the United States and those with whom they communicated; the extent of cooperation between U.S. private companies and the government in providing user and client data; information on U.S. espionage on Chinese computers; the joint operation between the NSA and the Government Communications Headquarters (GCHQ), the British counterpart to the NSA, to monitor the communications of political leaders attending the 2009 G20 Summit in London; the British mass surveillance scheme; the Internet domestic communications metadata collection scheme, among others. Author Lucas (2014) adds more to this: the "XKeyscore" program, revealed in July 2013; and the data chaining program, "Enterprise Knowledge System."

ternet.[12] After the leak of secret documents, Snowden, living in exile in Russia, began advocating for privacy, encryption, and a robust reform of current surveillance systems (Lee, 2015). Privacy and anonymity on the Internet are consistently and openly defended by the former NSA agent. In this regard, the TOR anonymous network has been elevated by him to the status of the most important privacy-enhancing technology of the current era (Ibid., 2015). Snowden's political stance is not limited to the desire for privacy for ordinary citizens alone. On the contrary, he advocates for other members of society: from those living under authoritarian regimes to professionals committed to reporting and factual accuracy, including political dissidents, whistleblowers, activists, and more. Although the actions of these individuals take place in the abstract realm of cyberspace, their consequences have implications for concrete reality. This demonstrates the political nature of the TOR communication channel in the 21st century. Understanding its functioning, as well as the actions of the various agents operating within it, allows an examination of how power relations are configured in the digital realm today—and, once again, with implications for concrete reality.

Thirdly, our approach aims to analyze the diffusion of power within the context of the TOR anonymous network. This network, by definition, falls under the structure of knowledge, as it is this structure that deals with "the channels by which beliefs, ideas and knowledge are communicated—including some people and excluding others" (Strange, 1988, p. 119). For this reason, and for the purpose of defining the scope of our research, we will analyze the diffusion of power through this structure. It is therefore important to understand both the focus of our analysis and the origins of structural power—two distinct points. While the focus of this research's analysis of diffusion of power rests on the structure of knowledge—which we believe is best suited to explain the reality of the TOR network and the actors operating within it—the structural power, as conceived by Strange (1988), remains a product derived from the four primary structures, to varying degrees. Thus, we believe it is possible for the focus of analysis to be on one of the structures without compromising conceptual meanings. Strange herself, at times, focuses her analysis on different structures when addressing the diffusion of power.[13]

Fourthly, we believe that this research contributes to academic studies on the theme of diffusion of the power in two ways: first, by bringing the theme into the cyber context; and second, by operationalizing the concept in a way that aids analyses of diffusion of

[12]The nonprofit organization Electronic Frontier Foundation (EFF), founded in 1990, is a leading advocate for civil liberties in the digital world and is currently battling the NSA in U.S. courts over the agency's surveillance of Internet infrastructure (Tummarello, 2016). In court, the EFF argues that the NSA violates the Fourth Amendment of the U.S. Constitution by copying and searching data collected from the Internet backbone within the United States (Maas, 2014).

[13]For example, Strange (1996) focuses on the Italian Mafia within the security structure. The Mafia competes with the Italian state for positions within the security structure. Similarly, she acknowledges that the Mafia's structural power is derived, to a greater or lesser extent, from all four structures—whether through providing physical protection to members and allies, trading illicit goods and services, offering credit to interested parties, or accessing knowledge and information networks.

power. Strange's works (1988, 1996) did not provide variables that could at least guide the direction of analyses on diffusion of power—how it occurs and to what extent. We believe that constructing variables that can at least delineate the analysis is relevant. Therefore, we will work with three variables during our investigation of diffusion of power within the context of the TOR low-latency anonymous network: authority, control, and outcomes. The methodology involving these variables will be described in the methodological section of this introduction.

Fifthly, we justify the investigation of the TOR network, the selected journalistic media, and the actors presented in this research. Within the context of the networks that make up the Dark Web, the TOR network is considered the largest in terms of nodes and users, as well as being perceived as having the most sophisticated cryptographic technology (Moore & Rid, 2016, p. 15). Moreover, we aim to use alternative journalistic media in the form of online newspapers to build the database on which we apply the variables described above. The selection of these newspapers was based on the *Top 10 Online Newspapers Worldwide Ranked by Unique Visitors*, published in 2012 by ComScore, a U.S.-based company headquartered in Virginia that conducts various analyses related to the Internet domain (ComScore, 2012). Finally, the agents selected for the analysis of the three variables were those who: (1) could be considered part of the knowledge structure, according to Strange's (1988) definition; and (2) actors whose operations took place through the TOR anonymous network.

The sixth and final justification relates to the author's personal motivations. These motivations can be summarized as an affinity for the themes of computing, information systems, and technology in general. During childhood, the author learned programming languages and, for the first time, was able to build a website on the World Wide Web (WWW). This experience led her to pursue studies in Computer Science, which were not completed due to her enrollment in Civil Engineering. Her interest and affinity for the Exact Sciences have been long-standing. Both fields were left behind when she began and completed her undergraduate studies in International Relations at the Federal University of Santa Catarina, earning her degree in February 2015. Her final undergraduate project (TCC), though brief, focused on the "Deep Web" and the "Dark Web." The TCC was supported by three justifications: the latent interest in Technology and Information Systems, especially the world of the Internet; the activist movements in the cyber domain such as Anonymous, WikiLeaks, the TOR Project, and Edward Snowden's revelations about global communication surveillance carried out by the Five Eyes members, which had political implications for the international scenario; and, finally, the growing concerns regarding the marginalization of these topics within the field of International Relations (IR). In 2016, she enrolled in the Graduate Program in International Relations at the Federal University of Santa Catarina with the intention of continuing her studies on the Diffusion of Power and the Dark Web. In 2017, she published the book *Deep&Dark Web:*

The Internet You Know Is Just the Tip of the Iceberg through Alta Books company.

This research is, above all, an attempt to analyze the forces and movements that occur in the cyber domain and reverberate in international political economy and in the daily lives of millions of people around the world.

1.3 Objectives

This dissertation works with one general objective and five specific objectives.

1.3.1 General

The general objective of the research is to understand how, and to what extent, the TOR network increases the diffusion of structural power in the 21st century. To enable the achievement of this general objective, the following specific objectives are proposed.

1.3.2 Specific

1. To examine the theoretical aspect of structural power that fundamentally diverges from traditional approaches to power in International Relations (IR);

2. To propose the operationalization of the concept of diffusion of power, developed by Strange (1996), through three ordinal qualitative variables;

3. To describe the historical, theoretical, and technological aspects that support and accommodate the anonymous TOR network within the cyberspace universe and distinguish it from other communication channels;

4. To analyze the database—composed of subjects from the structure of knowledge selected through newspaper articles—in order to assign values to the variables representing the three dimensions of power that confirm its diffusion;

5. To evaluate, through the previously described specific objectives, how and to what extent the TOR network increases the diffusion of power in the 21st century.

1.4 Methodology

The methodological starting point of this dissertation is the literature review. Initially, we start with a holistic view of the theme of "Science", "Technology", and "International Relations" and the positioning of this research within the aforementioned theme. Subsequently, we map the discussion on the Internet and International Relations in order to investigate the issues already addressed by scholars in the field regarding the cyber

domain and correlate them with this research (as presented in the introduction of this dissertation). We conducted an extensive search on "Power" and "International Relations" to examine how the theoretical framework related to power is configured as an approach within the discipline. Next, we observed how the element of "Diffusion of Power" is addressed by the theoretical framework and other authors in the field—aiming to outline distinctions and similarities. The theme of this research, Dark Web, is situated in cyberspace, and for this reason, we sought to identify the worldwide computer network as its own domain. To achieve this, we explored the literature on the "Origin of the Internet" in its technical aspect to gather knowledge about its operationalization and functioning. Consequently, we understood from the literature on the Deep Web the different nuances of the World Wide Web, among which the Dark Web is configured as just one of the categories. Finally, for the purpose of understanding the specificity and technological nature of the low-latency anonymous TOR network, we examined the literature on the Dark Web and TOR in order to provide the basic inputs through which we conducted the analysis of diffusion of power.

Below is a table composed of the literature review.

Table 1.1: Literature Review

Categories	**Literature on the subject**
Science, Technology and International Relations	SKOLNIKOFF, 1993; WEISS, 2005; KRIGE; BARTH, 2006; MATTHEWS, 1997; BUILDER, 1993.

Categories	**Literature on the subject**
Internet and International Relations	NYE, 2011; LANDAU, 2013; SCHEUERMAN, 2014; BAKIR, 2015; WALSH, MILLER, 2015; MURATA, ADAMS, PALMA, 2017; BRUNN, 1998; DERIAN, 2003; CASTELLS; CARDOSO, 2005; NISSENBAUM, 2005; BERENGER, 2006; WALSH; BARBARA, 2006; FARRELL, 2006; MICHALSKI; GOW, 2007; CLARKE; 2009; LIBICKI, 2009; CORNISH et al, 2010; ROSS, 2011; LAWSON, 2012; CHOUCRI; GOLDSMITH, 2012; KALLBERG; THURAISINGHAM, 2012; KRAMER, 2012; HATHAWAY, 2012; MILLS, 2012; TIKKRINGAS, 2012; HURWITZ, 2013; JUNIO, 2013; DEIBERT, 2013; DEMCHAK; DOMBROWSKI, 2013; VAISHNAV; CHOUCRI, 2013; MUELLER; SCHMIDT, 2013; ROCHE; BLAINE, 2014; CANABARRO, 2014; CEPIK; CANABARRO; BORNE, 2014; CEPIK; CANABARRO; BORNE, 2015; JAJODIA et al, 2015; SCHREIER, 2015; SCHNEIDER, 2016; SIEDLER, 2016; CHADWICK, COLLISTER, 2014; LANDAU, 2014; LUCAS, 2014; SCHEUERMAN, 2014; TOXEN, 2014; BAKIR, 2015; BRANUM, CHARTERISBLACK, 2015; LYON, 2015; MERCK, 2015; NOCETTI, 2015; QIN, 2015; SALVO, NEGRO, 2015; GURSES, KUNDNANI, HOBOKEN, 2016; MURATA, ADAMS, PALMA, 2017; TUMARELLO, 2016; CASTELLS, 2001.
Power and International Relations	PORTER, 2013; WRIGHT, 1995; DE JOUVENEL, 1957; BALDWIN, 2013; HENDEL, 1953; WALTZ, 1979; WALT, 1987; MOUL, 1989; CLAUDE, 1989; GUZZINI, 2000; SCHWELLER, 2006; KAUFMANN, LITTLE, WOHLFORTH, 2007; LITTLE, 2007; BROOKS, WOHLFORTH, 2008; WENDT, 1999; MORGENTHAU, 1948; SHEHAN, 1996; POLLARD, 1923; PAUL, 2004; WALTZ, 1990; MEARSHEIMER, 2001; SIMONDS, EMENY, 1937; LASSWELL, KAPLAN, 1950; NAGEL, 1975; DAHL, 1961; BACHRACH, BARATZ, 1962; LUKES, 1974; WENDT, 1992; HOPF, 1998; BARNETT, DUVALL, 2005; GUZZINI, 2007; KEOHANE, NYE, 2011; BALDWIN, 1995;
Diffusion of Power	BUILDER, 1993; NYE, 2011.

Categories	**Literature on the subject**
Internet Origin	FINKLEA, 2015; CASTELLS, 2001; NAUGHTON, 1999; BARAN, 1964; LAKSHMAN, MADHOW, 1997; CERUZZI, 2003; ASPRAY, CERUZZI, 2008; BANKS, 2008.
Deep Web	BERGMAN, 2001; FIDÊNCIO, MONTEIRO, 2013; SHERMAN, PRICE, 2001; BECKET, 2009.
Dark Web and TOR	SHERMAN, PRICE, 2001; FIDÊNCIO, MONTEIRO, 2013; BECKET, 2009; GEHL, 2016; CHERTOFF, SIMON, 2015; DEVINE, EGGER-SIDER, ROJAS, 2015; FINKLEA, 2015; ROCHE, 2016; ZULKARNINE et al, 2016; GHAPPOUR, 2017; MOORE, RID, 2016; DINGLEDINE, MATTHEWSON, 2005; PACHENKO, PIMENIDIS, RENNER, 2008; EDMAN, SYVERSON, 2009; CHAABANE, MANILS, KAAFAR, 2010; HOPPER, VASSERMAN, CHAN-TIN, 2010; LI et al, 2010; LI et al, 2011; ALSABAH, BAUER, GOLDBERG, 2012; MOGHADDAM et al, 2012; EDMAN, SYVERSON, 2009; LOESING, MURDOCH, DINGLEDINE, 2010; ELAHI et al, 2012; MCCOY et al, 2008; DINGLEDINE, MATTHEWSON, SYVERSON, 2007; AKHOONDI, YU, MADHYASTHA, 2012; MITTAL et al, 2011; MOGHADDAM et al, 2012; ALSABAH, BAUER, GOLDBERG, 2012; DUNGHEL et al, 2010; JOHNSON et al, 2013; FIFIELD et al, 2012; EDMAN, SYVERSON, 2008; HORSMAN, 2017; THOMSON, 2017; SCHULZE, 2017; BUCHANAN, 2017; SANDVIK, 2017; BIDDLE et al, 2011.

The theoretical framework of this dissertation is based on the works of the British scholar Susan Strange, which directly and indirectly address the phenomenon of the diffusion of power: *States and Markets* (1988) and *The Retreat of the State* (1996). From this theoretical framework, the need arose to systematize its content in the form of three distinct and complementary dimensions that make up the phenomenon of the diffusion of power: authority, control, and outcomes. These dimensions are implicitly present in Strange's works—but not as formal dimensions per se; rather, they serve as relevant elements for the construction of the analytical framework through which the author's global political economy vision is solidified. The diffusion of power is a phenomenon that occurs separately in each of these three dimensions.

The element of "authority" is interpreted through the lens of the concept of power. On rare occasions, Strange (1996) uses the term "power" when discussing the phenomenon of the diffusion of power, preferring instead the term "authority." When examining the

term 'authority' in her work, we notice a duality of interpretation attached to it: on some occasions, the term is seen as the institution, entity, or subject that embodies the expectation of power (being authority); on others, it is viewed as synonymous with power, or more precisely, with the ability to affect outcomes in such a way that the subject's preferences are imposed (exercising authority). In the first chapter, we aim to substantiate the reasons that indicate the existence of this duality and provide more detailed considerations about how these "authorities" manifest.

In this dimension, Strange discusses the effects of power arising from the presence or involvement of an authority—without the need for the authority to act, operate, or perform activities. Strange (1996) argues that this conception of power finds its origins in feminist approaches. Within a specific context, the presence of a figure understood as authority can be representative of power—and produces effects that are felt and perceived by other figures within that context, leading to consequences. To illustrate, the author addresses the relations between men and women and the inherent power of the male presence in the social context.[14] Furthermore, the presence of authority can emanate from its peers, recognizing three possible scenarios: that the authority is perceived as stronger, has remained the same, or has weakened.[15] We will discuss these ideas in detail

[14]Especially regarding this notion that power can act merely through presence—and not solely through actions—Strange offers some considerations about this type of power, which she discusses as being "structural", or rather, as a product of the dynamics of established structures (this includes the feminist approach, because power originates from the structural dynamics established in the social context of the patriarchy). She affirms: "A second general point is that 'power over' need not be confined to outcomes consciously or deliberately sought for. Power can be effectively exercised by 'being there', without intending the creation or exploitation of privilege or the transfer of costs or risks from oneself to others, for instance. This recognition of unconscious power is one contribution that gender studies has surely made to international political economy. Male partners may not wish or intend the control they have over outcomes affecting their female partners. But as many women are acutely aware, the social structures within which the partnership exists will make sure that such power exists. [...] This is where the distinction between what I have called relational power and structural power is relevant. In relations with others, it is much harder to think of power being exercised by one party over another unconsciously, without deliberate intent. But when you think of power in terms of power over structures, it is easier to understand that relations existing within those structures are affected, even though it may be inadvertently. The same is true of the power of United States government agencies over outcomes in the international system." (STRANGE, 1996, p.26)

[15]The perception of peers regarding authority—whether it is increasing, decreasing, or indifferent—is an idea indirectly addressed in Strange's 1988 work. The author provides several examples and I quote: "Without the productive power to supply food and capital goods for the reconstruction of European industry, and without the financial power to offer credits in universally acceptable dollars, the United States could not have exercised the power over the recipients of Marshall Aid that it did. Nor was American structural power based only on dominance of the security structure, the production structure and the financial structure. Its authority was reinforced by the belief outside America that the United States fully intended to use its power to create a better post-war world for others as well as for its own people. [...] Moral authority based on faith in American intentions powerfully reinforced its other sources of structural power. [...] A very different example of the power derived in part from the force of ideas would be that exercised within and beyond Iran after the fall of the Shah by Ayatollah Khomeini and his followers. The idea that the Shah, out of greed and lust for power, had fallen captive not only to a foreign country but to a culture and a materialistic belief system alien and inimical to traditional Islamic values had contributed powerfully to the collapse of his government and his own exile. But the power of the ayatollahs in defending and promoting Islamic virtues would have been constrained if they had not

in Chapter One, which focuses on the dimension of authority.

The "control" dimension appears frequently in Strange's works (1988, 1996) when discussing the operationalization of objects within primary structures. She often states that actors positioned in primary structures have power when they control aspects relevant to influencing outcomes in the economic-political scenario (Ibid., 1988). However, the controller of the object influencing outcomes is not necessarily the authority. In the first chapter, we identify various examples from Strange's work where actors within primary structures control objects deemed relevant for influencing outcomes.

The "outcomes" dimension is fundamental in Strange's literature because it determines the authority and control of actors: altering the status quo indicates power, while its preservation may indicate a lack of power.[16] This dimension encompasses both structural power (indirect) and relational power (direct).

In sum, Strange's works indicate that the diffusion of power operates through the three dimensions of "authority", "control", and "outcomes".These dimensions culminated in three ordinal quantitative variables present in our database, compiled from journalistic articles, which underpin our analysis of diffusion of power.

Our methodology is structured as follows: we will outline the three variables used in the diffusion of power analysis, explain their operationalization and scope, discuss the selection of journalistic articles for our database, identify the actors derived from these articles, and detail the process leading to our analysis of diffusion of power through three dimensions.

The independent variable is the TOR Network and the dependent variable is "diffusion of power". Our hypothesis is that the TOR Network enhances diffusion of power in the cyber domain. This research focuses on "how" this diffusion is possible and "to what extent" it occurs.

---

also gained control over the state and the armed forces sufficient to confirm their authority both within the country and beyond. Undoubtedly, the power of ideas was indispensable but it could only be used to affect outcomes in conjunction with military capability and economic resources." (STRANGE, 1988, p.32) I argue this excerpt highlights how moral and ideological authority can reinforce structural power, and how peer perception plays a crucial role in legitimizing and maintaining that authority.

[16] We argue that the absence of change does not always indicate an absence of power. Denying access to information, for example, demonstrates power by the actor who withholds it. Strange (1988) highlighted this concept as "negarchy", referring to power derived from resisting changes to the status quo. A classic example is the system of "checks and balances" that operates within the legislative, executive, and judicial branches of government. The ability of one branch to prevent excessive influence from another is indicative of its power. Another example from this research is the Tor Project, which exercises power by resisting digital surveillance over users and messages within the anonymous TOR network. This exercise of power affects outcomes by preventing surveillance, but it does not alter the status quo, as the status quo is the absence of surveillance. A change in the status quo would mean a new reality where digital surveillance is effectively conducted.

1.4.1 Variables "authority", "control" and "outcomes"

It is known that when discussing the diffusion of power, Strange (1996) did not use variables that could substantiate the phenomenon being studied. Her methodology, identified by her as "functionalist", examines the various functions of authority in political economy and raises questions about "who", or "what", would be exercising these functions or responsibilities—and, furthermore, with what effects on the outcomes (STRANGE, 1996, p.42). Although she did not approach the phenomenon from the perspective of operationalization, we believe that constructing ordinal quantitative variables is an important attempt to aid in the interpretation of the phenomenon. These variables are able to, at the very least, guide our analytical approach in relation to the diffusion of power.

Based on the reading of her work, our understanding of the diffusion of power is as follows: diffusion of power occurs when an actor has sufficient authority within a primary structure, at either the local or global level, to control an element that is capable of affecting the outcomes. In other words, their control over this element is decisive in determining the outcomes.[17] According to Strange (1996), the diffusion of power helps explain the rise of market power over the nation-state—or more precisely, the rise of the power of non-state actors who operate within each of the primary structures, and sometimes at the intersection of them (secondary structures). Her approach underscores the relevance and strength of non-state actors in the international system and highlights the urgency of addressing them in academic research to better understand international practice. For this reason, she distances herself from the discipline of International Relations—which is almost exclusively concerned with the state actor—and inaugurates International Political Economy, which encompasses non-state actors operating transnationally within the global political economy.

The table below systematically presents the three variables adopted in this research (first column), their scope of action (second column), and plausible values (third column).

Table 1.2: **The Diffusion of Power's Variables**

Variables	**Scope of Action**	**Ratings**		
Authority	Trust of peers and stakeholders	Decrease (-1)	Stability (0)	Increase (+1)
Control	Exercise/operation of the element	None (0)	Partial (+1)	Absolute (+2)
Outcomes	Impact on the status-quo	No change (0)	Change (+1)	-

Source: Author.

The first column, "variables," identifies the three variables of the diffusion of power

[17] For instance, she points out that the State holds control over the Armed Forces, which at times act in a way that influences the outcomes so that the preferences of the State take precedence over others. The control over the Armed Forces (and other structures) underpins the State's supreme authority within the security structure. And although the State faces rivals (for example, organized crime—sometimes referred to as "the parallel state") within the security structure, it still remains within this structure as the leading authority. (STRANGE, 1988).

phenomenon: authority, control, and outcomes.[18] The second column, "scope of action," presents the meaning or the underlying idea behind each variable, i.e., the scope of action of the variable. The third column, "ratings", represents through maximum and minimum values all the possibilities encompassed by each variable. For example: the "authority" variable has as its scope the trust of peers and stakeholders. This trust can decrease, remain stable, or increase. If a decrease is observed, based on the analysis of the journalistic article, the "authority" variable will be assigned the value "-1". And so on. The ratings for each dimension are based on the works of Susan Strange. Through them, it was noted that in situations where she mentions authority, she often analyzes whether a particular authority is in decline, growing, or stable. At other times, Strange (1988) indicates the importance of controlling resources that can impact results. And on several occasions, she emphasizes the importance of outcomes in determining the authority, control, and power of an actor. The foundation supporting the existence of the variables, scope of action, and ratings presented in this table is explained in Chapter One of this research and is backed by the literature of Susan Strange.

The first variable, "authority," refers to the sense of trust conferred by peers and stakeholders.[19] We can say that something or someone possesses sufficient authority within a structure when their peers grant them trust, whether formally or informally. In other words, before anything else, we need to identify the agent/actor in question as a local or global authority within at least one of the four primary structures identified by Strange (1988). If this is possible, the explanatory sequence of the variable follows. Otherwise, we cannot associate the actor with the "authority" variable. Let us consider an example.

A dentist has authority over dental matters because their professional council has granted them this authority through membership. They also have authority over these matters because the university from which they graduated conferred upon them a bachelor's degree, which allows them to enjoy certain legal prerogatives—including this authority. A drug trafficker has authority over drug transactions in a region because their peers, other drug traffickers, or stakeholders, such as consumers of the product, have granted them this trust. While the dentist is a formal authority, the drug trafficker is an informal authority. This "authority" can increase (in the case of a dentist, this happens when they conduct in-depth research on topics in their field, becoming a specialist in a specific subject); decrease (when the same dentist commits serious errors in the practice of their profession, leading to fewer clients as trust in their work diminishes; if the severity of the error is confirmed, they may be expelled from the professional council and have their legal prerogatives suspended); or remain stable (when the dentist does not become

[18]These variables are representative of the dimensions of the diffusion of power. In turn, these dimensions originate from the works of Strange (1988, 1996), which serve as the theoretical framework for this thesis.

[19]Strange uses the term "reliability".

a specialist in any specific subject but also does not commit errors in their professional practice—that is, they simply maintain their level of authority in the exercise of their professional activities).

An actor has power when they possess authority over something. This authority may have been granted through formal or informal means. Let us examine two examples to illustrate this. To demonstrate formality, we will use the example of sovereignty in the International System (IS). Sovereignty is a power exercised in the IS because it is formally recognized by the actors that compose it, or rather, by the peers of the state (state actors) and stakeholders (non-state actors). Regarding informality, consider the example of a drug trafficker in a region. The local population grants them authority based on community belief, either because they provide security in exchange for the ability to market their products or because they are excessively violent in the region, and the community submits to them out of fear of retaliation. Similarly, the US dollar is a currency with power that extends beyond the United States' borders because other states informally grant it authority when they use this currency in their commercial and financial transactions.

When the "authority" variable increases, we assign it a value of "+1"; when it decreases, we assign it a value of "-1"; and when it remains stable, we assign it a value of "0," as there is no change. This variable, therefore, can take integer values ranging from "-1" to "+1" (including the value "zero")—depending solely on the context of the situation in which the authority in question is found and the analysis derived from this context.

The second variable, "control," refers to the sense of exercising or operating a specific object relevant to achieving influence over outcomes. Again, we must first identify whether the agent has control over the object in question. If this can be ascertained, the explanatory sequence of the variable follows. Otherwise, we cannot attribute the "control" variable to the agent.

An actor has power when they have control over something relevant to achieving their desired outcomes. This power is the ability to alter the status quo. They may not be a formal or informal authority; however, if they have the capacity to control this relevant object, then they possess power over the outcomes. This would be the case, for example, of a military pilot in command of a combat aircraft. They do not possess authority; they are an instrument of operation for the Armed Forces to which they are subordinate. However, when, while flying over a region, they are ordered to release the bombs stored in the aircraft, this pilot has the choice to launch the bombs or not. At that moment, they have control over the object relevant to influencing the outcomes: the bombs. During this period, this soldier has power. Their actions can alter the status quo (e.g., not launching the bomb) if they so choose.

Something, or someone, only controls an object if they perform or operate actions to

that end—whether directly (themselves) or indirectly (using another person or mechanism). The "control" variable, when present, determines the degree of operation over the object: none, partial, or absolute. When this variable cannot be attributed to the agent in question, we say that the agent has no control over the specific object and assign the value of "none," which corresponds to "0," as their control is nonexistent. If the agent has partial control, they will receive the value of "+1." And if they have absolute control, they will be assigned the value of "+2." This variable, therefore, can take integer values ranging from "0" to "+2"—depending solely on the degree of control exercised by the agent in question.

The third and final variable, "outcomes," concerns the sense of "impact on the status quo." And, when it comes to the cyber domain, it is relevant to consider the "effects on reality"—the domain in which the actors are situated. Relevant outcomes are those that impact the real geographic plane—not the virtuality of the cyber domain. After all, an outcome only has meaning if it affects some aspect of the reality in which the actors are embedded. Any outcome in the cyber plane will only be taken into account if it also impacts the real geographic plane. A virtual game for leisure can have different outcomes for the players involved. For example, Player A might finish in first place. However, this outcome has no impact on the real geographic plane, as it is played for pleasure. If, by chance, the game took place within the context of a national championship, the first-place finish would certainly have some impact on Player A's real plane: monetary compensation, a prize, or a title.

An actor can also have power when their actions, with effects on the real geographic plane where the other actors are situated, alter or reinforce the status quo.[20] This is the case of a player in virtual games within a championship. When they compete against the world champion, they have neither authority nor control over the game. However, when they change the outcome (by defeating the world champion, for example), they acquire power (now, they themselves are the world champion). Not altering the outcome (the world champion remains the world champion)—that is, reinforcing the status quo—is also a way of allowing their opponent to maintain the power they already possessed.

The "outcomes" variable can indicate a change in the status quo or its lack of change. If it indicates a change, we assign the value "+1" because the status quo has been altered. If it does not indicate a change, we assign the value "0" because the status quo remains unchanged. This variable, therefore, can take integer values ranging from "0" to "+1" (including "zero," evidently)—depending solely on the analysis of the change in the status quo in question.

It is necessary to point out that our understanding of the operationalization of the

[20]As mentioned earlier, the power derived from reinforcing the status quo is related to the idea of "negarchy," or the force that arises from the denial of changes to the status quo. Strange (1996) reflects on "negarchy" in her work.

phenomenon of the diffusion of power does not concern the gain, stability, or loss of **absolute power** but rather the **level of power**. These are different things. When an actor experiences a loss in their level of power, they lose some power. They do not necessarily lose all their power. But to lose some power, they must have some power to begin with. This is why the situation of having no power and, furthermore, losing a level of power cannot occur. There is no negative power. Now, if an actor experiences stability in their level of power, this means there is neither gain nor loss of power. The actor simply maintains the same level of power they previously held. If they had no power, they remain with none. If they had some power, they retain the same "amount" of power. Their level, wherever it may be, remains unchanged. Finally, if there is a gain in the level of power, this indicates that the actor has necessarily gained some power. If they had none, they now have some. If they already had some, they now have even more—their power is reinforced and reaffirmed.

Finally, we need to make two observations regarding the operationalization of the concept adopted in this research. First, we do not propose that this operationalization, along with the variables, serves as a definitive guide to the diffusion of power. However, we believe it can support a perceptive analysis of the gain, loss, or stability of power in the International System (IS), according to the approach of International Political Economy (IPE). The central idea of this operationalization is to track the journalistic articles selected in this research, in which the actors' actions are carried out via the anonymous TOR network. We hope this operationalization aids in the analysis of each agent: whether they are losing, gaining, or maintaining the same level of power. Each case can only be evaluated individually, and its context must be respected. The assignment of values to the variables allows, for example, statistical correlation analyses, which, although not used in this research, provide inputs for various analyses. We are also aware that the operationalization of the phenomenon should not be a rigid guide on the subject. Second, the assignment of values to each actor will be based on perception—a subjective characteristic. Each actor, derived from the journalistic articles, will be analyzed through the variables discussed here to frame the perception of the diffusion or power in the context of the TOR network. The actors, who comprise the database of this dissertation, will be identified and discussed in the next section.

1.4.2 Selection of News

The search for analytical inputs has an investigative documentary nature, as it was conducted using documents preserved within private journalistic institutions. According to Gill (1991), this type of research has advantages as it is considered a "rich and stable source of data", does not imply high costs, and does not require contact with research subjects. Pádua (1997, p.62) further argues that documentary research is conducted

using contemporary or retrospective documents, considered scientifically authentic (not fraudulent), and has been frequently used in the social sciences.

We utilized alternative media—more precisely, online newspapers—to compose the reality framework on which the analysis of the diffusion of power was conducted. Riffe, Lacy, and Fico (2008) discuss media research and point out that the scientific method corresponding to "the systematic assignment of communication content to categories according to rules, and the analysis of relationships involving those categories using statistical methods" is called quantitative content analysis. This research method involves a series of techniques, including theoretical literature examination and the development of representative coding categories—aimed at reflecting differences between contents. Its application to mass communication content, such as newspapers, is based on the initial premise that the researcher seeks to develop a social science-based approach through empirical observations and measurements. In other words, there is sufficient suspicion to investigate "theoretical traits" in a specific practical context and thus propose explanations or relationships between different concepts (RIFFE; LACY; FICO, 2008). Regarding this, Riffe, Lacy, and Fico (2008) provide an example:

> If members of an ethnic minority, for example, voice concern that they are underrepresented in news media content (in terms of their census numbers), a researcher may propose that racism is at work or that members of the ethnic minority are underrepresented in those occupational groups that serve more often as news sources in the news. Each of these interpretations or explanations involves different concepts that can be “operationalized” into measurement procedures, and each can be tested empirically, as researchers did in the content analyses highlighted previously. (RIFFE; LACY; FICO, 2008)

The present research involves the operationalization of concepts and empirical analysis through the documentary investigation of journalistic articles and categorical measurements—therefore, it employs the scientific method of quantitative content analysis as presented by the aforementioned authors.

Our investigation was limited to the ten most-visited English-language online newspapers, as presented in the justification section. (COMSCORE, 2012).

The British newspaper *Mail Online* is the most accessed by users worldwide, closely followed by the American *The New York Times* and, again, a British newspaper, *The Guardian*. Two Chinese newspapers (*People's Daily Online* and *Xinhua News Agency*) and one Indian newspaper (*Tribune Newspaper*) are among the ten largest newspapers by user clicks worldwide—although the list is dominated by Western newspapers[21]. According to the ComScore (2012) report, *Advance Digital* is listed in the last position. Despite

[21]It was not possible to obtain any results for the term “Tor Network” in the newspaper *Xinhua News*

Table 1.3: **The Ten Largest Newspapers in the World by Clicks per User (in Millions)**

Rank	Country	Newspaper	Unique Visitors/Month (millions)
1st	UK	Mail Online	50.067
2nd	USA	The NY Times	48.695
3rd	UK	The Guardian	38.931
4th	India	Tribune Newspapers	35.862
5th	China	People's Daily Online	33.026
6th	UK	Telegraph Media Group	30.083
7th	China	Xinhua News Agency*	29.987
8th	USA	Washington Post	26.007
9th	USA	Hearst Newspapers	24.174
10th - Advance Digital (Group of 13 Newspapers) - 22.340 million visitors			
	USA	Alabama Local News	http://www.al.com
	USA	Cleveland OH	http://www.cleveland.com
	USA	Mississippi and Gulf Coast	http://www.gulflive.com
	USA	Le High Valley	http://www.lehighvalleylive.com
	USA	Mardi Gras	http://www.mardigras.com
	USA	Massachusetts Local News	http://www.masslive.com
	USA	Michigan Local News	http://www.mlive.com
	USA	New Jersey Local News	http://www.nj.com
	USA	New Orleans, LA Local News	http://www.nola.com
	USA	Oregon Local News	http://www.oregonlive.com
	USA	Central Pennsylvania Local News	http://www.pennlive.com
	USA	Staten Island NY Local News	http://www.silive.com
	USA	Syracuse NY Local News	http://www.syracuse.com

Source: comScore MMX, Worldwide, Age 15+, Oct 2012.
*Chinese News Agency.

being classified as a newspaper, it comprises a conglomerate of thirteen American newspapers. In total, the ranking of the ten largest newspapers in the world by user clicks, compiled by ComScore (2012), consists of 22 newspapers with active URLs.

To build the database for this research, we accessed the "archives" section (a publicly available database) of each of the listed newspapers and searched for the expression "tor network" (in quotation marks). With the exception of China's official news agency (*Xinhua News Agency*), all other newspapers returned a list of search results.[22] In total, 302 newspaper articles appeared as results for the search term "tor network." Of these,

Agency, the official news agency of the Chinese government. The search returned some page display issues, appearing to enter a "loop"—when the user makes a request to access the server unsuccessfully, and the procedure repeats indefinitely.

[22]Instead of returning results for the search of the cited term, the newspaper "Xinhua News Agency" repeatedly attempted to access the server but failed to display the results page. For this reason, it was not possible to identify the number of results for the search term "tor network" in the news archives.

only 195 actually dealt with the TOR anonymous network—190 were original articles, while 5 were duplicates.[23] In summary, out of the initial 302 newspaper articles, only 125 simultaneously addressed topics related to the knowledge structure.

Thus, we sought non-state actors who had some degree of social recognition regarding the possession of information and/or knowledge (Strange does not differentiate between these two terms by definition) that were responsible, in some way, for storing information, or controlled the channels through which this information was communicated. Within the universe of 190 original articles related to the TOR anonymous network from the ten largest newspapers by user clicks worldwide, we found that 125 articles discussed non-state actors who met the aforementioned definitions. In some articles, more than one non-state actor was mentioned—so we opted to call "occurrences" the situations involving a single non-state actor and "article" the journalistic reports that could discuss one or more actors. In 14 articles, we identified two actors. Each actor was treated as a unique occurrence deserving analysis.[24] In total, we identified 139 occurrences eligible for analysis—these became the 139 rows in the database for this research. In other words, each row in the database represents a single occurrence involving only one non-state actor positioned within the knowledge structure. Through the newspaper articles, we observed that these actors carried out specific actions via the TOR anonymous network.

Table 1.4: **Number of Occurrences for Analysis (2007-2017)**

Occurrences*		**N**
Results for "Tor Network"		302
Content Unrelated to "Tor Network"		105
Content Related to "Tor Network"		195
Originals		190
Actions via Other Means		15
Actions via Tor Network		177
Content Unrelated to the Knowledge Structure		52
Content Related to the Knowledge Structure**		125
Content with 2 Actors per Article		14
Content with 1 Actor per Article		111
Repeated		5
Total	$111+(14+14)=139$	139

Source: Author.
*Situations extracted from newspaper articles composed of a single actor.
**Includes articles composed of actors who are part of the knowledge structure.

[23]The search, which was definitively used in the research, was conducted in the second half of February 2018. The first search was conducted in May 2017.

[24]Therefore, the focus of our research was on the number of occurrences — not the number of articles. For detailed information, see "Appendix 8 — Articles and Occurrences for Analysis by Year."

Defined by Strange (1988), the knowledge structure encompasses belief, established knowledge, and the communication channels through which beliefs, knowledge, and information are conveyed. These are the three aspects of the knowledge structure. This structure also determines what knowledge is discovered, how it is stored, and who communicates this knowledge—using which means, to whom, and under what conditions (STRANGE, 1988).

The anonymous TOR network is a communication channel through which beliefs, knowledge, and information are securely transmitted. Moreover, the actors originating from the 125 occurrences are embedded within the knowledge structure because they engage in actions related to the discovery, storage, and communication of information and knowledge through the TOR network. According to Strange (1988), actors positioned within the knowledge structure occupy decision-making roles. On this, she observes:

> [...] Power and authority are conferred [...] on those who are acknowledged by society to be possessed of the 'right', desirable knowledge and engaged in acquisition of more of it, and on those entrusted with its storage, and on those controlling in any way the channels by which knowledge, or information, is communicated. [...] More than other structures, the power derived from the knowledge structure comes less from coercive power and more from consent, authority being conferred voluntarily on the basis of shared belief systems and the acknowledgment of the importance to the individual and to society of the particular form taken by the knowledge — and therefore of the importance of the person having the knowledge and access or control over the means by which it is stored and communicated. (STRANGE, 1988, p.121).

Actors within the knowledge structure have the capacity to influence outcomes through structural power, which, within this structure, operates less coercively and more through consent. Using this framework—journalistic articles related to the anonymous TOR network and actors positioned within the knowledge structure—we selected occurrences to construct the database. It is from this database that we analyze the diffusion of power across three dimensions: "authority," "control," and "outcomes."

The column "COUNTRY" displays the name of the country where the newspaper is based; "NEWSPAPER," the name of the online newspaper; "ARTICLE TITLE," the title of the examined article; "AUTHOR," the name of the author (or editor) of the newspaper article; "YEAR," the month and year of publication in journalistic media; "ACTOR," the actor or subject derived from the newspaper article and through which variables are examined; "CATEGORY," the thematic group in which the subject is categorized; "PEERS," the actor's peers and stakeholders; "AUTHORITY," the degree of authority of the subject in the given newspaper article;[25] "OBJECT," the object controlled by the

[25]The degrees of authority are: increasing, stable, and decreasing. The corresponding values are:

actor according to the article; “CONTROL,” the degree of control the subject has over the object in the article;[26] “STATUS-QUO,” the status quo before the actor’s intervention; “EFFECT ON REALITY,” whether the actor’s actions in the article had real-world effects; and “OUTCOMES,” the degree of change in the status quo in the real world caused by the subject in the given newspaper article.[27]

Table 1.5: **Database Columns for This Research**

Column	**Information**
COUNTRY	Country where the newspaper is located.
NEWSPAPER	Name of the newspaper responsible for the article.
ARTICLE TITLE	Title of the article.
AUTHOR	Author of the article.
YEAR	Year of article publication.
ACTOR	Actor whose actions are described in the article.
CATEGORY	Thematic group of the occurrence.
PEERS	Identification of peers and interested parties.
AUTHORITY	Identification of the "AUTHORITY" variable in the occurrence. Receives values: "-1" for decreasing authority, "0" for stable authority, and "+1" for increasing authority.
OBJECT	Control object of the actor identified in the occurrence.
CONTROL	Identification of the "CONTROL" variable in the occurrence. Receives values: "0" for no control, "1" for partial control, and "2" for absolute control.
STATUS-QUO	Presents the status-quo of the occurrence.
EFFECT ON REALITY	Identifies whether the actor’s actions have an effect on reality. If positive, assigns "YES". If negative, assigns "NO".
OUTCOMES	Identification of the "OUTCOMES" variable in the occurrence. Receives values "0" for no change in status-quo and "1" for change in status-quo.
REPEATED ARTICLES	"YES" to indicate that the article from which the occurrence was extracted is present in another row of the database, and "NO" to indicate the article’s originality.

Source: Author.

The "CATEGORY" column was established by us and formulated to understand actors in groups of similar themes according to the journalistic articles. There are six categories:

- **Digital Security**: involves themes related to digital security.

“+1”, “0”, “-1”

[26] The degree of control can vary between “none,” “partial,” and “total,” with the corresponding values being “0,” “1,” and “2.”

[27] The degree of outcomes varies between “change” and “no change” in the status quo. The corresponding values are “+1” and “0.”

- **Surveillance Circumvention**: refers to themes related to shielding against digital surveillance.
- **Journalism & Whistleblowing**: relates to themes of journalism profession and whistleblowing.
- **Online Marketplace**: digital markets operating on the anonymous network.
- **Privacy**: involves news specifically about user data.

In total, we identified 25 non-state actors, which we categorized into the six aforementioned groups:

Table 1.6: Non-state Actors by Category

Category	**Actors**
Digital Security	Dan Egerstad, Iranian Cyber Army, Freedom Hosting, Onion Ransomware, SimpleLocker Android Malware, Ransomware
Surveillance Circumvention	Tor Project, Facebook
Journalism & Whistleblowing	Chelsea Manning, Edward Snowden, Harold T. Martin, WikiLeaks, X-Net Group, ProPublica, Strongbox, SecureDrop System
Online Marketplace	Silk Road, Silk Road 2.0, Silk Road 3.0, Alphabay, Evolution, Sheep Marketplace, Farmer's Market
Privacy	Doxbin

Source: Author.

From the newspaper articles, we extracted the necessary information to populate the database. Besides creating the categories composed of actors with similar themes, we also identified who were the peers and stakeholders interested in each actor's actions and activities. The "PEERS" column aims to identify the subjects whose degree of trust in relation to the actor increases, decreases, or remains stable. As we've seen, this trust degree is translated by the "authority" variable - hence the creation of the "PEERS" column, to provide basis for the "authority" variable. Additionally, we identified the relevant objects for achieving the intended results through the "OBJECT" column. The degree of control over the object exposed in this column translates into the "control" variable. Therefore, it was necessary to identify the control object.

The "STATUS-QUO" column seeks to identify the state of the situation prior to the subject's actions because it is from the change or maintenance of this state that we assign values to the "outcomes" variable. However, before assigning this value, we need to know whether the change or maintenance of the status-quo affects geographical reality, since

this research operates within cyberspace. If there is an effect on reality, we assign the value consistent with the change or maintenance of the status-quo. If there is no effect on reality, we assign the value "zero". Again, the filling of these fields is done based on the content of the newspaper articles.

In summary, the methodology used in this research employs both qualitative and quantitative approaches to analyze the specific objectives. The qualitative approach consists of examination of literature review;preparation and transcription of the database from alternative online newspaper sources; pre-analysis with floating readings; categorization; presentation of results.

The quantitative approach, on the other hand, focused on assigning numerical values to assist in interpreting the power diffusion in each dimension across the selected set of journalistic articles. The general methodological components were: inclusion of online newspapers for database structure; delimitation of the knowledge structure - excluding analysis of other structures presented by Strange (1988); definition of variables and their possible assigned values; period and form of data collection that composed the database.

For data analysis within the quantitative approach, the results are presented in tables, charts, graphs and descriptive statistics - through frequency calculations and relative percentages. Microsoft Excel 2010 was used for spreadsheets and calculations. Data analysis was performed through variable tabulation using descriptive statistics - with absolute and simple relative frequency. Using this method, we made considerations about the phenomenon of power diffusion in the context of the TOR anonymous network, a component of the Dark Web.

1.4.3 Database Composition for the Research

For comprehension purposes, we randomly selected a newspaper article to demonstrate how each information column was filled. The article is titled *Global Drug Survey findings: more people buying drugs online in the UK*, published on April 14, 2014 by *The Guardian*, based in the United Kingdom and authored by Ami Sedghi.

The article discusses the increase in online drug purchases in the UK and features the actor *Silk Road*, an online marketplace operating on the TOR anonymous network. According to the article, nearly 60% of respondents were aware of the Silk Road marketplace, while about 44% reported having visited the site. The peers and interested parties are private citizens.

Based on this article:

- We assigned the value "+1" (increasing authority) to the authority variable because more than half of respondents knew about the online marketplace, and the article stated that more people were buying drugs online in the UK. We interpreted that trust in the marketplace among its peers and stakeholders was growing.

- The control object of the Silk Road actor is the online marketplace itself through its webpage and Bitcoin payment mechanism. Therefore, for the control variable, we assigned the value "+2" (absolute control) since control over both the marketplace operations and payment mechanism is administered by a single actor - Silk Road itself. This control is neither dependent on nor shared with any other actor.

- We identified that the status-quo of the situation addressed by the mentioned newspaper article is the fixed number of people in the UK who consume drugs through online purchases. The Silk Road actor changes this status-quo by contributing to the increase in the number of people buying drugs online in the UK.

- This status-quo change has an effect on the real world because people are indeed consuming narcotics and illicit substances. For the outcomes variable, we assigned the value "1".

- Finally, the article in question is original - meaning an article with a single actor. There will be no other actor from this same article.

It is worth remembering that when assigning values to the variables, we also identified the peers and interested parties (authority); the relevant object for achieving desired outcomes (control); the status-quo, so we could examine whether there was any change (outcomes). These findings are fully available in the research database provided in the Dissertation Appendix.

1.5 Dissertation Structure

This dissertation is organized into three substantive chapters. The first chapter establishes the theoretical framework within International Relations (IR) that will inform the interpretation of results in the third chapter. The presentation progresses from broad conceptual foundations to specific analytical perspectives.

The first chapter comprises three principal sections. The opening section introduces British scholar Susan Strange, a seminal figure in IR and International Political Economy (IPE), providing biographical context and outlining her major contributions. The second section examines the nature of structural power through two classical IR lenses: the relational approach and the national elements approach. This dual analysis substantiates Strange's theoretical innovation regarding power concepts within IR—a departure from classical disciplinary approaches that constitutes the core of her scholarship. The third section presents Strange's framework of diffusion of power, which requires understanding both relational and structural power concepts as they operate within her structural analytical framework for IPE. This framework encompasses the economic and political structures governing people and services. We conclude the chapter with Nye's (2011)

considerations about power diffusion in the cyber domain from *The Future of Power*, complementing Strange's (1996) work which did not address cyberspace.

Chapter two focuses on the technological dimensions of information systems. The initial section discusses the technological foundations and historical development of the Internet. The second section analyzes the WWW architecture, distinguishing between the "Surface Web" and "Deep Web." Building on Sherman and Price's (2001) taxonomy, the third section classifies the "Deep Web" and situates the "Dark Web" within the broader Internet ecosystem. The chapter culminates with an explanation of the technical characteristics that distinguish the Tor network's low-latency architecture from other Dark Web networks. Tor's unique technical specifications enable operational scenarios impossible on conventional web platforms, making this network the foundational infrastructure for the diverse actors examined in this study.

The third chapter presents our analytical database and methodology for examining the diffusion of power through three operational dimensions: "authority," "control," and "outcomes." This tripartite framework operationalizes Strange's (1996) concept of diffusion of power. Our analysis assigns specific valuations to each variable, with final interpretations derived from value frequency distributions across actor groups. The chapter concludes by presenting key analytical findings.

The concluding synthesis integrates three core elements: (1) the theoretical framework, (2) the technological context, and (3) the database analysis employing our operationalized diffusion of power metrics. This integrated approach enables comprehensive examination of power diffusion phenomena within the cyber domain—specifically focusing on the Tor network ecosystem.

1.6 Final Considerations

Traditionally, International Relations (IR) emphasized two main approaches to power — relational power and material power.[28] The reflection on the international scenario through an analytical framework revealed a gap in power studies within IR discipline — since these approaches focused primarily on state-centric analyses. According to Strange (1996), this state-centric view is excessively restrictive as it does not correspond to the reality of the international system: transnational corporations and other non-state actors frequently exercise power that affects millions of people's daily lives, yet they remain ignored in academic analyses. As Strange herself noted:

> "What the notion of structural power in world politics, society and economy did was to liberate the study of international political economy from the

[28]Baldwin (2013) refers to these approaches as "relational" and "national elements of power," respectively.

so-called realist tradition in the study of international relations." (Strange, 1996).

Furthermore, she argued that power diffusion adequately explained the declining quality of state authority while other actors' authority was rapidly growing.

However, as Palan (1999) observes, Strange cannot be confined to a standard theory-practice dichotomy for two reasons: she was neither theoretical nor "empirical" in the conventional sense. Rather than being theory-oriented, Strange aimed to develop an analytical framework for exploring issues. This explains why *States and Markets* clearly presents the dilemma between theory and "theorizing", while lacking empirical rigor (Palan, 1999). We believe this same dilemma appears in *The Retreat of the State: The Diffusion of Power in the World Economy* (1996). Despite introducing innovative themes like the accounting profession and the Mafia in global political economy, the author provides neither methodological framework nor empirical evidence to substantiate power diffusion — at least by academic standards. This observation, however, doesn't diminish Strange's pioneering work in IPE. As Palan (1999) suggests, perhaps strict empirical rigor would have raised her concerns about detachment from reality. She explicitly invited researchers to develop theoretical and empirical work on non-state authorities and their impact on IPE's four structures:

"Like plants in nature, theories and explanations grow out of the dirt of observations of reality. The observations may not be 'scientific' in the sense that an experiment in chemistry can be objective. But they are not invented either. Getting your hands dirty with the nitty-gritty details of a technology, or with the decision-making processes of corporate strategies, or of ministerial policymaking, is a good way to test the abstractions of theory, and perhaps to develop alternate theory, or modifications of theories. Moreover, if you can illustrate a theory or a hypothesis with reference to a concrete situation, it often serves to explain more clearly the thrust of the ideas. That is part of the point of my rather scrappy descriptions of non-state authorities and how they affect power structures to be found in part II of the book. They may have been chosen somewhat at random, out of personal interest. But they are supposed to illustrate the theoretical propositions laid out in the earlier chapters. It is my sincere hope that these examples will serve to stimulate younger scholars to more innovative work, theoretical and empirical, on non-state authority in the international political economy. They are by way of being a signpost, pointing not along an open well-trodden track but rather into a mysterious forest of the unknown. Just where the path will lead, I am not at all sure. That is the nature of exploration — and its appeal to the mentally adventurous." (STRANGE, 1996, p.xvi).

Responding to this invitation, this thesis explores studies on knowledge structure to examine non-state authorities and the diffusion of power in cyberspace, specifically within the TOR anonymous network. We pursue this through two approaches: first, by explicating three dimensions of structural power that, while not formally treated as such in Strange's works, are implicit in her writings; second, by operationalizing the diffusion of power concept through these three dimensions to enable empirical analysis. Our objective is to contribute academically to IPE studies.

Chapter 2

Theoretical Framework

The objective of this chapter is to present the theoretical foundation within the field of International Political Economy (IPE) that will serve, in the third chapter, as the analytical basis for interpreting the diffusion of power in the context of the anonymous network The Onion Router (TOR), as reported in journalistic documents.

In this first chapter, we begin from a broad perspective of the traditional concept of power in International Relations (IR) and move toward the alternative conception developed by Susan Strange (1988), which she termed *structural power*. This alternative concept is presented with particular attention to the structure of knowledge. Such structuring aims to provide sufficient theoretical foundations for explaining the phenomenon of *diffusion of power*—introduced subsequently as part of this dissertation's theoretical framework. The phenomenon of *diffusion of power* is grounded in the notion of structural power.

Next, we explore the three dimensions that, according to our interpretation, are essential for understanding the phenomenon of diffusion of power: *authority*, *control*, and *outcomes*. These three dimensions are present in Strange's works (1988, 1996), although they were not explicitly formulated as such by the author. This section will therefore provide the necessary elements for assessing the existence and scope of power diffusion within the TOR network (which is part of the knowledge structure)—an analysis developed in the third chapter of this dissertation.

Finally, we briefly present what the IR literature on power has argued in the cyber domain, focusing on the concepts of *cyber power* and *power diffusion* developed by Joseph Nye (2011).

In summary, this first chapter is organized around the following thematic topics: a brief biographical introduction to Strange; a mapping of traditional debates on power in IR, aimed at highlighting the theoretical gaps explored by Strange—which led to her break with IR literature and the development of her structural analytical framework in IPE; a presentation of structural power and the structure of knowledge; a discussion of the phenomenon of power diffusion; an exploration of the three dimensions—*authority*,

control, and *outcomes*—and their respective connections with the phenomenon of *power diffusion*; and, finally, an examination of the current IR literature on power in the cyber domain.

2.1 Biography and Contributions of Susan Strange

Born in 1923 and graduated in Economics from the London School of Economics (LSE) in 1943, Susan Strange—considered by many the most influential figure in British international studies—was almost solely responsible for establishing the field of International Political Economy (IPE) in the twentieth century. She began her career in journalism before moving into international studies. According to Brown (1998), her late entry into academia helped her remain largely unaffected by ego-driven temptations, as the academic world is shaped not only by learning but also by its institutions and prestige.

The erudite Strange was a resounding voice advocating the fusion of two major disciplines, Economics and Politics. She believed this fusion could foster the emergence of a new field within International Relations. On this point, Brown (1999) argues that there are two fundamental reasons that motivated her to advocate for the merging of these areas in the global context:

1. With few exceptions, she often believed that either economists neglected the role of power in global affairs or were overly confident in their abstract and formal economic models of the real world;

2. Most political scientists appeared excessively impressed by military forces and might, and, for this reason, attributed more power to institutions than they actually possessed.

Brown (1999) also emphasizes that any understanding of Strange's work must begin with her most evident trait: eclecticism. This characteristic forms the foundation of the interdisciplinarity of the IPE discipline itself.[29]

During roughly ten years, from 1965 to 1976, Strange was a full-time researcher at Chatham House. It was during this period that she published her manifesto *International Economics and International Relations: A Case of Mutual Neglect* (1970), in which she advocated a new analytical approach for International Relations, understood as the amalgamation of Economics and Politics, in order to grasp the reality of interactions and forces

[29]Some of her works include: *Sterling and British Policy: A Political Study of an International Currency in Decline* (1971); *Casino Capitalism* (1986); *States and Markets* (1988); *Rival States, Rival Firms: Competition for World Market Shares* (1991, co-authored with John M. Stopford and John S. Henley); *The Retreat of the State: The Diffusion of Power in the World Economy* (1996); and *Mad Money: When Markets Outgrow Governments* (1998).

in the global context.[30]

In any case, Strange's efforts to make the field of IPE visible and to attract scholars interested in conducting conjunctural and systemic analyses are undeniable. Scholars note that she generated something very close to an alternative theory of International Relations, although she was neither recognized as a theorist nor did she claim this label herself (Palan, 1999; Cohen, 2016). Her studies on power demonstrate her intellectual approach to issues on the agendas of IR and Economics. Cohen (2016) emphasizes that the element of power is central to any explanation of the character and dynamics of the global economy. Tooze and May (2002) consider Strange's analyses of power to constitute the most significant contribution to the field of IPE. The erudite Strange thus stands out as one of the major figures in the disciplines of IR and IPE.

2.2 Power According to Traditional Approaches in IR

International Relations inaugurated the field of study whose domain belongs to what has conventionally been called "international politics" (Porter, 2013, p.4). The American political scientist Quincy Wright (1955) defined "international politics" as the effort to influence "major groups in the world so as to advance the purposes of some against the opposition of others."[31]

The political scientist at Princeton University and emeritus professor at Columbia University, Baldwin (2013), argues that all "politics" involve the element of power, even when other elements are discussed. From this, we can infer that international politics also deals with the element of "power"—both from the inception of IR as a discipline in 1919 and in studies of international political events predating that time (such as the

[30]From the manifesto arose a conference under the auspices of Chatham House, which brought together groups of scholars from various fields in the U.S. and the U.K. in 1972. This conference, in turn, led two years later to the formation of the International Political Economy Group (IPEG), organized by Strange within the British International Studies Association (BISA), also formed through her own initiatives (Brown, 1999).

[31]This explanation has, as a consequence, a significant political connotation that encompasses the international sphere. However, it does not imply that only states are involved in politics. Other actors are also relevant. Political philosopher Bertrand de Jouvenel (1957) suggests that those involved in politics go beyond politicians themselves, party members, or even social movements with explicitly political objectives. He emphasizes two fundamental points: first, an action becomes political when the assistance of others is a necessary condition for an individual to achieve their goal; second, as a consequence, politics occurs when a project requires the support of another's will. In IR, politics is frequently treated as the domain of rulers and high-level government officials. It is in this aspect that Strange differs from the conventional conception of politics in IR. The British scholar assumes, similarly to Bertrand de Jouvenel, that politics involves not only rulers but all those who act based on the will of others, in order to make assessments regarding the political dynamics of power. For this reason, she is able to observe non-state actors as political subjects and include them within the analytical framework she develops to understand IPE. Both state and non-state actors can be examined through this framework, which differs from traditional IR approaches.

Peloponnesian War, widely analyzed within the discipline).[32]

The element of "power" is widely associated with the Realist theoretical current, although it is not exclusive to it. On this point, Wendt (1999) notes that a defining feature of Realism is indeed the assertion that the nature of international politics is shaped by power relations. However, he also emphasizes that this feature is neither unique nor exclusive to Realism.[33]

According to Baldwin (2013), two traditions dominate the study of power analysis in International Relations: the "national elements of power" approach and the "relational power" approach. The former treats power as a resource, while the latter identifies it as a relationship, whether actual or potential. We will examine these two approaches below in order to understand the landscape of power studies that preceded the development of IPE.

2.2.1 The National Elements of Power Approach

The "national elements of power" approach conceives power in terms of *resources*, something that an actor can possess. In other words, these resources are treated as if they were power itself (Baldwin, 2013, p. 277). There is no consensus regarding what these resources are, though some interpretations suggest they consist of the measurable elements that make up a nation—such as *territory size*, *population*, and *level of wealth* (Ibid., p. 280).

This notion of power as property is embedded within theoretical currents that discuss the *balance of power* (Ibid., p. 281). According to Wright (1965), the term "balance of power" embodies the idea that changes resulting from relational political power can be *observed and measured* in practice—in other words, power is a resource that can be quantified. This is consistent with the concept of *possession*, *ownership*, or *control*, which lies at the core of the "national elements of power" approach.[34]

There are three theoretical currents that adopt this perspective: the *classical balance*

[32]The discipline is nearly a century old. Its origin is believed to date back to 1919, with the creation of the first chair for the study of international politics in the world—at the Department of International Politics of the University College of Wales, Aberystwyth (Schmidt apud Porter, 2013). In 2019, the University of Aberystwyth celebrated the centenary of the discipline, noting that the department's foundation was a "response to the extreme violence of the First World War, in which millions of people from various parts of the world lost their lives. This foundation constituted an intellectual response to a global event with a normative purpose: to understand the different facets of world politics (politics, law, economics, ethics) in order to mitigate organized violence" (Aberystwyth University, 2017, our translation from written portuguese back to english). Over the decades, the discipline progressed academically, promoting successive waves of theoretical phases: idealism, realism, behavioralism, post-behavioralism, pluralism, neorealism, rationalism, post-positivism, and constructivism (Schmidt, 2017).

[33]According to Baldwin (2013), despite debates on "power" in IR failing to produce a consensus, there is a basic conception of power that is most widely accepted: initially formulated by Dahl (1957), it is the idea that actor A causes (or has the ability to cause) actor B to take an action that B would not have undertaken without A's intervention. This is the conception of relational power.

[34]The term "balance of power" is widely debated in the IR literature, as different authors argue that it is excessively broad (Pollard, 1923; Sheehan, 1996; Baldwin, 2013). Baldwin (2013) points out that Morgenthau himself admitted using the term to convey four different meanings.

of power theory proposed by Hans Morgenthau (1948); *neorealism*, also known as *structural realism* or *defensive realism*, developed by Kenneth Waltz (1979); and *offensive realism*, formulated by John Mearsheimer (2001).

The Classical Balance of Power Theory

Hans Morgenthau is the most prominent exponent of the *classical balance of power theory*.[35] According to Morgenthau (1948), if we wish to determine the power of a nation, we must distinguish its elements into two major groups: those that are *relatively stable* and those that are *subject to constant change*.[36]

From Morgenthau's perspective, it is the responsibility of those in charge of a nation's foreign policy — as well as those who shape public opinion on international affairs — to correctly assess the impact of these factors on the power not only of their own nation but also of others. This directly relates to the idea of the *balance of power*.

Paul (2004, p. 4) observes that the balance of power theory is grounded in the notion that states pursue two main objectives: to *survive independently* and to *accumulate power* within an anarchical system. Without power, they risk becoming subordinate to the will of others, thereby losing security and prosperity. For this reason, anarchy is the driving force that compels states to increase their power: both security and physical survival cannot exist apart from the maximization of power. Within this context, competition for power becomes a logical outcome.

Weaker states, according to Paul (2004), may lose their security — or even cease to exist — when threatened by an alliance of stronger states. Thus, weaker actors tend to form coalitions in order to balance power against stronger ones.

These observations belong to what is known as the *classical balance of power theory*, which, according to Baldwin (2013), regards military strength as the core capacity to prevail in war, since it is discussed within an analytical framework that presupposes armed confrontation among states. Therefore, this theory's meaning is intrinsically tied to the military context.

[35]Nevertheless, the concept predates the twentieth century. It was already used by the Greek historian *Thucydides* in his attempt to explain the causes of the *Peloponnesian War*, as reported by David Hume (1742) in his essays. In any case, Michael Sheehan (1996) considers the notion of "balance of power" one of the most important ideas in history for two reasons: first, it is a key concept that helps scholars of International Relations understand the recurring patterns of state behavior under the shadow of anarchy; and second, it has served as a guiding principle for many statesmen.

[36]The first group includes factors such as geography and natural resources (e.g., food and raw materials). The second group comprises industrial capacity, military preparedness (including technology, quality of leadership, and the size and capability of the armed forces), population (distribution and demographic trends), national characteristics (intellectual and moral qualities), national morale (the degree of determination with which a nation supports its government's foreign policy in times of both war and peace, including the stability of morale and the quality of society and government), and the quality of diplomacy (which reflects the quality of government, the balance between resources and policy, and popular support). (MORGENTHAU, 1948).

Neorealism

Known as *structural realism* or *defensive realism*, **neorealism** was developed by Kenneth Waltz in his seminal work *Theory of International Politics* (1979). Among his key contributions, Waltz theoretically introduced the notion of a *structure* within the international system. According to the author, "any approach or theory, if it is rightly termed 'systemic', must show how the system's level, or structure, is distinct from the level of interacting units. [...] Only by doing so can one distinguish changes of structure from changes that take place within it." (WALTZ, 1979, p. 40). This structural conception is the theoretical element that distinguishes this school from its classical predecessor.

Neorealism conceives the political structure based on three assertions: (1) the *ordering principle*, or the way in which units are organized; (2) the *differentiation of units* and the specificity of their functions; and (3) the *distribution of capabilities* among units (WALTZ, 1979, p. 88).[37] Although the distribution of capabilities is a key element of neorealism, Baldwin (2013) notes that Waltz never explicitly defines what "capabilities" are, while simultaneously admitting that states could be ranked, for instance, from most to least powerful according to their capabilities. This allows for the interpretation that "capabilities" are, in essence, *resources of power*.

Offensive Realism

Offensive realism, in turn, emerges from John Mearsheimer's work *The Tragedy of Great Power Politics* (2001). The central idea behind this approach involves two possible modes of state behavior within the balance of power: a state may act either to *defend* the balance of power or to *undermine* it.[38]

This defense or "sabotage" of the balance of power is directly related to *fear*. According to Mearsheimer (2001), fear is grounded in three logics: first, the absence of a supranational central authority capable of protecting states from descending into armed conflict; second, the existence of military power, that is, the offensive capabilities of states; and third, the persistent uncertainty that dominates the international system, since states can never be fully certain about the intentions of others.

These three factors explain the pervasive fear among states within the anarchic international system. As a consequence, states internalize the idea that the more powerful they are relative to their rivals, the greater their chances of survival. From this, it follows that the best survival strategy is to become the *hegemon* of the international system,

[37] Waltz originally uses the term "capabilities". According to the Macmillan Dictionary (2017), the word *capability* has two meanings: first, "the ability to do something"; second, "the number of weapons, soldiers, etc., that a country has for fighting a war".

[38] A powerful state acts to defend the balance of power when the risk of change favors another state. Conversely, it acts to weaken the balance of power when the potential change benefits itself. (MEARSHEIMER, 2001, p. 3). Mearsheimer also argues that the structure of the international system "forces" states — even those seeking only security — to behave aggressively toward one another.

since no other state could seriously threaten a hegemon due to its overwhelming position of power (MEARSHEIMER, 2001, p. 3).

The three theoretical traditions within the discipline of International Relations mentioned above share certain commonalities as well as key divergences.[39]

According to Baldwin (2013), although the "national elements of power" approach remains present in the literature, it faces certain analytical challenges because it treats power as if it were itself a resource. If power is a resource — and resources are static — then what functions as a resource of power in one situation may not function in another, since context is ever-changing. Furthermore, resources are linked to potential power rather than actual power (BALDWIN, 2013).

Thus, the fundamental characteristic of the "national elements of power" perspective lies in the understanding that power can be measured through a state's resources. Additionally, it assumes that states are capable of translating power derived from their resources into clearly defined national objectives (SHEEHAN, 1996).[40]

2.2.2 The Relational Power Approach

The way in which the field of International Relations had observed power until then — through the "national elements of power" approach — changed around the 1950s, when power began to be conceived as the result of a relationship.[41] This is the central concept of the relational power approach. Instead of being grounded in the notion of possession, power now rests on causality (BALDWIN, 2013). This new relational understanding of power is also adopted by Strange (1996), who recognizes the existence of both relational and structural power — as will be discussed later.

[39]Hans Morgenthau, Kenneth Waltz, and John Mearsheimer all approach power from an essentially military perspective (BALDWIN, 2013, p. 283). Classical realism and offensive realism depict states as actors seeking to maximize power. However, for Morgenthau (1948), this pursuit stems from a desire for power in itself, while for Mearsheimer (2001), the maximization of power is a natural consequence of the anarchic international system in which states exist (BALDWIN, 2013, p. 283). Both defensive and offensive realism portray state objectives as derived from the structure of the international system. Waltz (1979) argues that the primary goal of a state is to maintain a sufficient level of security to ensure its survival, with no need to accumulate power beyond what is necessary. In contrast, Mearsheimer (2001) claims that the ultimate goal of the state is to become a "hegemon," gathering as much power as possible to reach that status (BALDWIN, 2013, p. 283).

[40]It is worth noting that, within realist perspectives, international politics primarily concerns the politics conducted among the Great Powers — those which Simonds and Emeny (1937) identified as States possessing sufficient military capabilities to effectively sustain the foreign policy determined by their own decisions. Realism does not concern itself with the politics of States that are not considered Great Powers. This is because Great Powers can afford the "luxury" of "waiting to see" how foreign policy unfolds, since their own capabilities — translated into military power — can ensure the implementation and maintenance of such political will.

[41]Baldwin (2013) explains that several scholars viewed the work of Lasswell and Kaplan (1950), *Power and Society*, as a revolutionary milestone in International Relations — precisely for presenting this new conception of power grounded in causality.

The relational power approach assumes that the behavior of actor A, at least partially, provokes a change in the behavior of actor B. It is therefore called "relational," as it operates through cause and effect within the context of a relationship between two actors. In this view, there is no notion of power derived from resources, capacities, or attributes of the State. Moreover, relational power comprises different dimensions. Baldwin (2013) explains that there are, at minimum, four: *scope*, *domain*, *weight*, and *costs*.[42] According to Jack Nagel (1975), when employing this relational power approach, it is necessary, at the very least, to specify the dimensions of "domain" and "scope."

There are two major milestones within the relational power approach: the Constructivist school and the "Faces of Power" debate. While Constructivism comprises three relevant studies — the theoretical foundation of the school by Alexander Wendt, the notions of identity and interest developed by Ted Hopf, and the interpretation of "polymorphous" power by Michael Barnett and Raymond Duvall — the Faces of Power debate encompasses three progressive stages, based on the idea that power has three faces. For Baldwin (2013), this was one of the most significant debates involving the concept of power in the twentieth century. Both milestones made important contributions to the understanding of relational power.

Constructivism

Wendt (1992) identifies the existence of social theories on interests and identities that had been neglected by the discipline of International Relations and incorporates them into a framework he calls "constructivism" — in order to emphasize the focus on the social construction of subjectivity.[43]

Ted Hopf (1998) notes that Constructivism brings alternative themes to the IR agenda: anarchy, balance of power, the relationship between state identity and interest, the elaboration of power, and prospects for change in global politics. Specifically regarding power, Hopf (1998) recalls that Constructivism argues that the notions of *material power* and *discursive power* are both necessary for understanding international affairs.

[42] "Scope" refers to the aspects of B's behavior that are affected by A, for example, economic aspects. "Domain" encompasses the set of actors subject to A's influence. "Weight" refers to the probability that B will be affected by A. "Costs" refer to the means through which B is affected by A, which may be symbolic, economic, military, or diplomatic. (BALDWIN, 2013, p.275).

[43] In 1992, Alexander Wendt published the article *Anarchy is what states make of it.* In this article, he observed that the debate between neorealists and neoliberals shares a common foundation — "rational choice". This assumption implies that scholars are automatically directed to ask certain questions instead of others, as there is no inquiry into identities and interests. These points are not pondered when discussing actors in International Relations. This means that processes and institutions may change their behavior, but the studies about them preserve their identities and interests — they are static, unquestioned. (WENDT, 1992). Wendt (1992) proposes two avenues of inquiry: first, that the answers to these concerns depend partly on how important the interactions among States are for constituting their identities and interests; second, that they also depend on how easily States' interests and identities change in response to systemic interactions (Ibid., p.423).

Indeed, States coexist within the international community and maintain relations of power, directly or indirectly. For Constructivism, it makes little sense to focus solely on the material, military, or coercive aspects when seeking to understand interactions among States and the formation of power balances. It is necessary to study the dimension of power that emerges from the relationships among them — relationships that are consolidated through conventionalized practices within the international system (while, for instance, Wendt seeks to understand why certain practices became conventions).

Despite their relevance, States are not the only actors in this system. This curious point reveals that some approaches within the IR discipline aim to bring other actors — beyond the State — into the scope of significant studies and research. Up until then, scholars were primarily concerned with the State and the power games of the international political arena.

The Americans Michael Barnett and Raymond Duvall (2005), in turn, interpret power as "polymorphous" — that is, it manifests itself in different forms.[44] They offer an explanation for why power has been treated, in IR, essentially under the theoretical umbrella of Realism (something that Strange also does).[45] For these authors (Ibid., p.45–46), power can be expressed in two forms: through interaction (that is, through cause and effect); or through the constitution of actors as social beings (in this case, power operates through social relations). They conclude that this conceptual distinction is very similar to the distinction about power in the literature of the field that discusses "power over" and "power to."

The Faces of Power Debate

Finally, the Faces of Power debate encompasses considerations regarding the first face, second face, and third face of power. The debate concerning the "first face of power" begins with the studies of Robert A. Dahl (1961) in his work *Who Governs? Democracy and Power in an American City*. In this study, Dahl (1961) seeks to understand who governs in the city of New Haven, in the state of Connecticut, in the United States. In short, the "first face of power" has one focus: to determine who has the power to put forth political proposals in the decision-making process of a given issue. The second face

[44]The four types of power formulated by them (Ibid., p.43) are: compulsory power, institutional power, structural power, and productive power. Compulsory power is power as relations of direct control interactions of one actor over another. Institutional power is the direct control that actors exercise indirectly over others through diffuse relations of interaction. Structural power is the constitution of the subject's capabilities in direct structural relation of one with another. And, finally, productive power is the socially diffuse production of subjectivity within systems of meaning and signification.

[45]The authors suggest that realists essentially treat power as a material resource of coercion whose purpose is to influence actor B to alter its behavior. According to them, the tendency to associate power with the Realist theoretical current in IR is due to the fact that realists are practically the only ones who address power directly. Without the existence of considerations about power in other spheres, Realism triumphs almost hegemonically when it comes to the Theories of International Relations. (BARNETT; DUVALL, 2005).

of power is associated with the studies of Bachrach and Baratz (1962): both argue that there are sets of issues that will never be brought to the decision-making table because, in the first face, certain issues were already taken as given. But there are others that are not selected. This neglect reflects the debate of the second face of power: the ability that power has to select which issues will be discussed in the decision-making process. Finally, the third face of power was presented by Lukes (1974) as the manner through which actor A causes a change in the behavior of B. There are different forms — A can affect B's needs, thoughts, desires, and even preferences. Lukes (1974) acknowledges the similarity of the third face of power with the studies of Antonio Gramsci on "hegemony" and Joseph Nye on "soft power."

2.3 The Break with the IR Theoretical Tradition

Both through the national elements of power approach and through the relational power approach, the unit of analysis addressed by traditional theoretical currents in IR had been almost exclusively the nation-state. For Strange (1996), this was troubling insofar as it distanced theory from the actual practice of everyday life: non-state actors proliferated in the IS with considerable authority over a range of issues.

When Morgenthau (1948) discussed the balance of power and introduced the view that power could be "measured," he was referring to the power of the State in the international arena: power is amenable to measurement based on a State's resources. Waltz (1979), in turn, understood the international arena through a defined political structure — with an ordering principle, differentiation of units and the specificity of their functions, and the distribution of capabilities among units. In this IS, States can be ranked according to the power they "possess," since power resources are the State's own capabilities. Mearsheimer (2001), for his part, revisited the idea of the balance of power, highlighting the privileged position of the State in this context of the IS. States are the agents that seek to defend their balance of power or to undermine it (if doing so favors them in some way).

In none of the theoretical currents within the national elements of power approach is the relevance of actors other than the State acknowledged. After all, since the elements are "national," these currents neither admitted nor concerned themselves with the existence of elements not attributed to the State. Thus, as sovereign, the State — besides being the sole "player" — also saw in anarchy the reason to secure itself as an independent entity capable of surviving in the IS. These currents did not explain, nor did they intend to explain, the development, the power, or the survival of transnational corporations or any other non-state actor with authority on the international stage. And yet, these currents remained the fundamental pillars upon which the discipline of IR was built — a discipline that, it bears recalling, discussed international politics without, until then, considering non-state political actors.

Shortly thereafter came the relational power approach. It made the observation of power more flexible because it acknowledged, for the first time in the field of IR, that power was not derived solely from national elements. Relational power arose from the conception of an idea of causality: it is the exercise of influence that A has over B so as to alter B's behavior in order to achieve outcomes desired by A. This conception of power broke with the earlier notion grounded in national elements. Whereas power had previously been viewed as a resource, an element of possession, the new approach sought to confer a causal meaning to power, derived from a relationship. But, similar to the national elements approach, analyses employing the relational power approach commonly treated international politics as the arena of States. Broadly speaking, both approaches lacked the recognition and explanation of the existence of power and authorities originating from the Market — or rather, from the private sector. It is here that Strange's contributions become evident. She recognized that, in practice, numerous non-state authorities held power over activities and people in the IS. On this point, she stated that "It seems to me that the powers of most states have declined still further, so that their authority over the people and their activities inside their territorial boundaries has weakened. Non-state authorities, meanwhile, have impinged more and more on those people and their activities." (STRANGE, 1996, p.xi).

How could Strange explain the existence, and the power, of non-state authorities in the IS based on a traditional IR literature? How could she discuss international politics without considering the dimension of non-state actors, recognizing them as authorities with power over activities and people on the international stage? By all indications, she could not. And for this reason, she broke with the discipline of IR to dedicate herself to the study of international politics from the field of IPE. Although there were some approaches that sought to address non-state actors, the fact remained that within the discipline of IR, the State persisted as the center of analyses on international politics. On this point, she stated:

> That [new realism] merely added new issues to the agenda of inter-state diplomacy and new bit-players to the cast of actors in international politics. It left the state and its concerns still always at the centre of the stage. It is the *always* that I now find unacceptable, and which leads me to feel that perhaps I have at last reached the final parting of the ways from the discipline of international relations. I have been involved with it now, as student, foreign correspondent and teacher over more than half a century. But I can no longer profess a special concern with international politics if that is defined as a study different from other kinds of politics and which takes the state as the unit of analysis, and the international society of states as the main problematic. (STRANGE, 1996, p.xv)

For Strange (1988), analyses of international politics needed to encompass the practices experienced in the international arena — and this included the existence of non-state actors and the power that these authorities exercised over people and activities. For this reason, she sought to ground her analyses on three fundamental premises:

> [...] Politics is a common activity; it is not confined to politicians and their officials. The second is that power over outcomes is exercised impersonally by markets and, often unintentionally, by those who buy and sell and deal in markets. The third is that authority in society and over economic transactions is legitimately exercised by agents other than states, and has come to be freely acknowledged by those who are subject to it. (STRANGE, 1996, p.12–13).

The first premise opens space for political considerations beyond the stage governed by national governments and international organizations — which includes the politics conducted by multinational enterprises, transnational corporations and organizations, and other authorities. The second premise indicates that power does not stem solely from political relations but also from economic and financial relations. Capital opens the opportunity for the exercise of power. The third premise removes the exclusivity of the State's authority over people and activities within its geographical borders. This last premise aims to dismantle, as far as possible, the wide gap between everyday practice and the theories and analyses produced in academic centers around the world. With these three premises in view, the reader can appreciate both the eclecticism of Susan Strange and the relevance of the "symbiosis" between the disciplines of Politics and Economics for the analyses of International Relations — after all, power and capital walk together on the global stage.

In what follows, we turn to the studies on "power" and "diffusion of power" that emerged in IPE from the work of the British scholar Susan Strange, in the late 1980s and mid-1990s. The reviews of the element of "power" discussed thus far help us understand the reasons why Strange (1988) formulated the notion of structural power and how it fits into the reading of power within International Relations. Strange's triumph (1988) was perhaps her contribution to the notion that power also resides in non-state actors within the context of the IS. To this end, Strange (1996) did not resort to the creation of an alternative theory of power that could account for new actors. According to Palan (1999), she employed her own eclecticism to create a framework from which analyses of the practical reality of the IS (and of the foundations that underpin the human condition) could be examined. This framework was conceived by her on the basis of fundamental human values as forms of social organization: wealth, security, freedom, and justice (STRANGE, 1988). In this way, Strange's approach to the element of power proceeds from a holistic perspective — which is why Palan (1999) believes that the concept of structural power cannot be used independently of the framework of the four structures

elaborated by her. After all, structural power does not emanate from the four structures (security, production, finance, and knowledge), but is rather the very articulation of elements originating from them (PALAN, 1999).

In the following sections, we have three objectives: (1) to define the four primary structures described by Strange (1988), with particular attention to the structure of knowledge; (2) to present the concept of structural power; (3) to describe the phenomenon of the diffusion of power. These subjects are found in two main works by the author: *States and Markets*, 1988, and *The Retreat of the State: The Diffusion of Power in the World Economy*, 1996. The latter work is considered by her as "an extension, or elaboration, of the same ideas about power and transnational relations that characterise the contemporary world scene." (STRANGE, 1996, p.x). The ideas on power and transnational relations are presented in the first work, *States and Markets*.

2.4 Structural Power

In 1988, Susan Strange introduced the concept of structural power in her work *States and Markets*. This concept emerges as an alternative interpretation of power to the existing concepts in the IR literature. For her, two forms of power are exercised within a Political Economy: relational power and structural power. However, even while recognizing the existence and exercise of relational power, she points out that structural power has had greater relevance in the IS.

Strange defines structural power and offers several considerations about it. She stated that:

> Structural power [...] is the power to shape and determine the structures of the global political economy within which other states, their political institutions, their economic enterprises and (not least) their scientists and other professional people have to operate. [...] In short, [it] confers the power to decide how things shall be done, the power to shape frameworks within which states relate to each other, relate to people, or relate to corporate enterprises. [...] Structural power is to be found not in a single structure but in four separate distinguishable but related structures. [...] These four, interacting structures are not peculiar to the world system, or the global political economy, as you may prefer to call it. The sources of superior structural power are the same in very small human groups, like a family or a remote village community, as they are in the world at large. The four sources, corresponding to the four sides of the transparent pyramid, are: control over security; control over production; control over credit; and control over knowledge, beliefs and ideas. Thus, structural power lies with those in a position to exercise

> control over (i.e. to threaten or to preserve) people's security, especially from violence. It lies also with those able to decide and control the manner or mode of production of goods and services for survival. Thirdly, it lies at least in all advanced economies, whether state-capitalist, private-capitalist or a mix of both — with those able to control the supply and distribution of credit. [...] Fourthly and lastly, structural power can also be exercised by those who possess knowledge, who can wholly or partially limit or decide the terms of access to it. This structural power in particular does not easily fit into the layer-cake, club-sandwich model because it may very easily lie in part beyond the range and scope of the state or any other 'political' authority. Yet its importance in political economy, though not easy to define or describe, is not to be underrated. (STRANGE, 1988, p.24–28).

Structural power originates from the four structures mentioned in the previous section. The structures do not emanate power; rather, it is through the articulation of elements arising from these structures that structural power is conceived. For this reason, both Palan (1999) and Brown (1999) do not consider Strange a theorist: she does not create an alternative theory; she provides inputs sufficiently capable of offering a worldview about actors (state or non-state) and their activities based on interrelated structures (themselves conceived from fundamental values of human organization). It is from this structural vision of the IS that actors relate to one another. This structural vision allows, above all, the inclusion of non-state actors in academic studies in IPE — something inconsistent with the discipline of IR up to that point. The relevance of these actors in Strange's work is considerable because (1) it reflects the political and economic practice found in the everyday reality of international affairs, where multinational enterprises (and other organizations or even individuals) maintain agreements and exert influence over governments, people, and organizations; (2) it demonstrates that, within each structure (security, production, finance, and knowledge), the State is neither the sole actor nor the most relevant one to the point of assuming the top position, the leadership, of the structure. On the contrary. In a later work, Strange (1996) acknowledges that the State assumes a leadership position in only one structure: security (STRANGE, 1996). In the remaining structures, the contemporary State is merely one of the relevant actors that exert influence and seek power — it is not the only one.

The four structures are not present solely in the international context. The conception of structural power is grounded in an analytical framework, or rather, a method through which diagnoses are made about the human condition as affected by social, political, and economic circumstances (STRANGE, 1988). Given that such circumstances also describe the local context, structural power is disseminated throughout the economic-political fabric at various levels. Indeed, for this reason, one can analyze, through the

conception of structural power, the human relations that occur in families, neighborhoods, or human tribes — provided that these relations arise from social, political, or economic circumstances.

Furthermore, we observe, from the quotation above, that structural power **falls upon** those who are in a position of **control** within the context of at least one primary structure (security, production, finance, and knowledge). On this point, Strange (1988) stated that:

> Structural power lies with those in position to exercise control over (i.e. to threaten or to preserve) people's security, especially from violence. It also lies with those able to decide and control the manner or mode of production of goods and services for survival. Thirdly, it lies — at least in all advanced economies, whether state-capitalist, private capitalist or a mix of both — with those able to control the supply and distribution of credit. [...] Fourthly, and lastly, structural power can also be exercised by those who possess knowledge, who can wholly or partially limit or decide the terms of access to it. This structural power in particular does not easily fit into the layer-cake, club-sandwich model because it may very easily lie in part beyond the range and scope of the state or any other 'political' authority. Yet its importance in political economy, though not easy to define or describe, is not to be underrated. (STRANGE, 1988, p.26–28).

In other words, it is about having control over an object within at least one primary structure — in the local and/or global context. Whether on a neighborhood street, over a neighborhood, or nationally or globally. Moreover, Strange (1988) indicates that the possessor of control over a structure (at its macro or micro level) can exercise power without apparently placing direct pressure on others to make a decision or choose among alternatives. And this is possible because structural power, despite being less "visible" (than material power, for example), is still present.

However, many may question: if structural power derives from articulations originating from four interrelated structures — and not exclusively in an individual manner — how can it fall upon an actor that exercises control over an aspect of at least one structure? Strange does not provide an answer, but we may venture a conjecture. Structural power was represented, metaphorically, by Strange as a tetrahedral pyramid whose faces represent the primary structures (security, production, finance, and knowledge). And, despite originating from the dynamics of elements arising from the structures, it can be "observed" from one of the faces of the tetrahedron, or rather, from one structure. In other words, although it is understood through the four structures (which complement and relate to one another), there exists the possibility of observing structural power originating specifically in the context of one of the structures. It does not originate in isolation

from a single structure, but the analytical focus of structural power can be directed toward one of the structures. It is possible to rotate the pyramid so as to examine each of its faces in detail.[46]

2.5 The Four Primary Structures

Susan Strange (1988) defined four primary structures: the security structure; the finance structure; the production structure; and the knowledge structure.[47]

The security structure is the "framework of power" created through the provision of security by some human beings for other human beings (Ibid., p.45). What follows is an example that we have taken the liberty of formulating based on the invitation to creative stimulation made by the author herself in the context of her works.

Imagine a prehistoric era in which human beings wandered in bands across the earth and needed to protect themselves from threats posed by the climate, animals, diseases, geographical hazards, other human groups, and so forth. The individual within the group who was capable of providing security for the other(s) — who, for instance, were being threatened by an enemy — gains "structural power" within this "framework of power." This individual is capable of affecting outcomes (by protecting the band from the enemy, the outcome is that the group is saved — as opposed to another possible outcome, which is the death of the band) in such a way that their preference (the salvation of the band) takes precedence over the preference of the other (the death of the band). Control over the group's security confers upon this "savior" individual structural power, which originates through the security structure. Their band, and the enemy band, will come to see this individual as a "powerful" agent and will think twice: before launching violent incursions against them (security); when producing some good that may be of interest to them (production), since there is a risk to the physical integrity of the one who produces the good (after all, to obtain the good, the powerful individual may threaten them); and when providing "loans" or credits in the form of food, clothing, and so on, due to the risks to physical integrity. The relationship between this actor and their own band, and between this actor and rival bands, is altered — even if the "savior" individual is not aware of it.[48] And this relationship is altered because, once they are seen as a "powerful"

[46] See "Appendix 1 — Pyramid Representing Structural Power."

[47] There are also secondary structures: transnational transport systems, the trade system, energy supply systems, and the transnational welfare and development system (Ibid., p.139). The British scholar acknowledges that the selection of these structures is somewhat "arbitrary in the sense that it would be equally logical to include some other secondary structures." (Ibid., p.139). The main characteristic of these secondary structures is that, although they are frameworks of action within which choices are made based on value preferences, they are also secondary to the four primary structures of security, production, finance, and knowledge. When it comes to structural power, she formulates the analogy of the pyramid.

[48] Note here the contribution of gender studies to IPE, as mentioned by Strange (1988).

agent, their mere presence will be capable of operationalizing this power.

At the micro level, this can happen both in the context of prehistory, in small human groups, and in the context of the outskirts of a city in the current era. At the macro level, this occurs both from the domestic standpoint, when the State gathers unto itself the legitimate use of force in society, and from the international standpoint, when it seeks to alter the balance of structural power among actors. According to Strange (1988), in the context of the current international system, the security structure is conceived around the institution of the State, even though the State does not act in isolation within the system (STRANGE, 1988).

The production structure can be defined "as the sum of all the arrangements determining what is produced, by whom and on what terms." (STRANGE, 1988, p.64). That is to say, from the perspective of Strange's IPE, the production structure is responsible for creating "wealth." When this structure changes, "big changes are apt to follow in the distribution of social and political power, and sometimes the nature of the state and the use of authority over the market." (Ibid., p.64). It is natural that such changes occur, since the production structure lies at the heart of the organization of life in society. Increasingly, the production structure in the global context is characterized by transnational enterprises. On this point, Strange (1988) stated that "the nature of the global production structure [...] is the combined result of state policies and of market trends, of management strategies and changing technology." (Ibid., p.80).

The finance structure is defined according to the actors capable of creating or denying the granting of credit to others, without whom no advanced economy can function (STRANGE, 1988). If we observe this issue from the micro level, we perceive that "the power to create credit implies the power to allow or to deny other people the possibility of spending today and paying back tomorrow," and at the macro level, "all the arrangements governing the availability of credit plus all the factors determining the terms on which currencies are exchanged for one another." (STRANGE, 1988, p.90). Reflexively, the one who has control over credit is capable of directly or indirectly affecting the scope of the choices available to others.

The knowledge structure is defined by Strange (1988) as follows:

> [...] A knowledge structure determines what knowledge is discovered, how it is stored, and who communicates it by what means to whom and on what terms. [...] So power and authority are conferred on those occupying key decision-making positions in the knowledge structure — on those who are acknowledged by society to be possessed of the 'right', desirable knowledge and engaged in the acquisition of more of it, and on those entrusted with its storage, and on those controlling in any way the channels by which knowledge, or information, is communicated. (STRANGE, 1988, p.121).

This structure is related to knowledge that is produced, discovered, stored, and communicated. Note that Strange (1988) does not draw conceptual distinctions between "knowledge" and "information," so long as the unit in question is considered socially relevant. Those who possess relevant and desired knowledge, and also those who in some way control the channels of communication and storage of such information, are conferred structural power originating from the knowledge structure. Beyond power, they are also conferred authority.[49] These two elements, power and authority, are conferred upon these individuals by virtue of occupying important positions within the structure, because in addition to being decision-makers, they are also recognized as holders of the knowledge desired by society (which, therefore, has value for the social organism). We may assume some examples originating from the knowledge structure, such as researchers, content creators, library science professionals, information systems specialists, computer scientists, and so on — in short, the class of professionals (and prominent figures in a given area of knowledge) who are related, directly or indirectly, to the production, communication, and storage of knowledge (or information) considered socially relevant. These figures are considered "authorities" within the knowledge structure. And to be an authority, it is necessary, first, that the actor actually possesses the said relevant knowledge; and second, that such knowledge be considered important (STRANGE, 1988).

Some examples presented by Strange (1988) highlight past actors who succeeded in the accumulation of structural power, originating mainly from the knowledge structure, over the years: the Catholic Church during the medieval period and the scientificist State of the twentieth century. The Catholic Church held authority and power because, among other important points, it controlled the means of communication (which spanned all of medieval Europe) through which knowledge was transmitted, in the form of sacred books and literacy in the sacred Latin language. Those who were granted access to the storage of knowledge — the sacred books guarded by the Church — needed, in addition to access, knowledge of the language in which the information was inscribed. Note that it was the Catholic Church that controlled, during the medieval era, the means of communication and storage — in addition to investigating discoveries and denying access to knowledge to other individuals. The scientificist State, on the other hand, was identified by Strange (1996) as the institution that assumed some of the Catholic Church's responsibilities regarding the knowledge structure (such as the growth of the educational system that allowed access to education in schools and universities) and invested in technical innovations (through which new knowledge was discovered in various fields, especially Physics), thereby giving rise to intellectual property rights (STRANGE, 1988).

The knowledge structure is also somewhat different from the other structures for

[49]This semantic distinction between "power" and "authority" in this quotation from Strange is relevant for understanding authority as a dimension in its own right. This will be discussed at a later point.

several reasons: (1) Strange (1988) affirms that the power originating from the knowledge structure is understandably diffuse; (2) it is a power she describes as "unquantifiable"[50]; (3) the power derived from the knowledge structure is also grounded in the denial of access to knowledge; (4) it is a power more associated with consent than with coercion — unlike the other structures; (5) there must exist social recognition that a given piece of information is considered important — so that the person holding this knowledge is also considered relevant to society (STRANGE, 1988).

Finally, we must understand that the structures are not static; they are dynamic and subject to changes and developments. On this point, Strange (1988) acknowledges that, of all the structures, the knowledge structure is the one undergoing the most rapid changes at the end of the twentieth century.[51] And although she did not write specifically about the Internet when making considerations about the knowledge structure, Strange recognized the relevance of the information revolution occurring at the end of the twentieth century.[52] In particular, she highlighted the importance of the combination of three technological areas that were undergoing major changes: widely available and low-cost computer systems; large-scale satellite communication systems in orbit; and the digitization of language, which opens the potential for the dismantling of linguistic barriers among human groups (STRANGE, 1988). And, in the end, she concluded that the interaction among the structures suggests very important political conclusions: the ongoing

[50]My interpretation of this is that in the other structures, the power originating from them is still amenable to quantification — even if roughly. In the finance structure, for example, it is possible to have a sense of the "quantity" of power through a banking analysis of credit granting. From a micro perspective, one can gain a sense of structural power by examining how much was "lent" to an individual. This financial amount determines the purchasing power of the individual who received the credit and offers an idea of the intensity of the creditor's power. In the production structure, by contrast, we can have a reasonable idea of the "quantity" of power through how much was produced (or left unproduced), how much was manufactured. In the security structure, this perception of "measurable" power occurs through the analysis, for instance, of the size of armies, the quantity of a State's military resources, the number of nuclear warheads. The possession of 50 nuclear warheads versus "none" is an indicator, broadly speaking, of the power that certain States hold in the provision of security or the threat of violence. At the micro level, we observe the number of members comprising a street gang and the quantity of resources they possess both to protect and to threaten third parties. But in the knowledge structure, it is understandably difficult to quantify "how much" knowledge an individual, or group of individuals, possesses. Knowledge and information do not translate into numbers of books, articles, journals, newspapers, and so on, since these numbers do not automatically signify absorbed and communicated knowledge. This is the difficulty of measuring structural power originating from the knowledge structure. We should note, however, that Strange (1988) indicates that control over the channels of communication (and also storage) through which information, knowledge, and beliefs are communicated also confers structural power. Thus, the one who allows or denies others access to these channels of communication holds power. This point is perhaps the only one that permits an illustration of the "quantity" of power originating from the knowledge structure: a global private company that, through the use of technology, enables millions of people to communicate using its communication channels (e-mails, servers, chat platforms, shared "office" suites, etc.) and decides to alter its access policy holds structural power, as it directly affects the options of action available to its clients. Even so, it is merely an indicator of power.

[51]Strange writes about the primary structures in the context of her 1988 work, that is, also at the end of the twentieth century.

[52]Susan Strange passed away in 1998, and thus did not write specifically about the digital information systems that culminated in the rise of the commercial Internet.

technological innovations were resulting in the global unification of goods and services (Ibid., p.130). Although the world had already experienced the unification of markets, these were limited by transportation systems. The new dynamic, grounded in microelectronics, is different: the new means of communication allow information to be accessible to buyers and sellers globally — and they also allow purchase and sale decisions, as well as the execution of those decisions, to be carried out instantaneously. Therefore, this entails innovative political and economic consequences (Ibid., p.131).[53]

Strange (1988) demonstrates awareness of her limitations regarding the knowledge structure. In part because she recognizes that the power derived from the knowledge structure is the most neglected of all (security, production, and finance) in the studies of social psychologists, philosophers, technology specialists, and others. As such, there is little input for analyses that depart from the knowledge structure. And in part because the change occurring in the knowledge structure is the fastest among all structures and, for this reason, the results are not yet clear. But, despite this, she asserts that there is sufficient evidence to sustain that the knowledge structure is undergoing at least three broad transformations.

The first of these has to do with the very relevance of the knowledge structure. Strange (1988) affirms that at the end of the twentieth century, the knowledge structure is considered so important that competition among States in the IS can be understood as a competition for the leadership of this structure. In the past, this was not the case: States competed for territory. And the competition for territory occurred because the production of wealth (and, therefore, the acquisition of power) depended on land and natural resources. The twentieth century altered this competitive conception: States seek the leadership of cutting-edge technological development (Ibid., p.136). According to her, there has long been popular recognition that "knowledge is power," but IR and IPE theorists have yet to absorb this reality within academia.

The second development refers to the increase in asymmetry among States as political authorities in the acquisition of knowledge and access to it (Ibid., p.137). In the IS, States present themselves as sovereign and equal political authorities — but access to and the acquisition of knowledge do not occur on equal terms.

The third development, less explored by the author, concerns new distributions of power, social status, and influence beyond state borders — by reason of the knowledge

[53]Some of these economic and political implications include: the relevance of information for the production structure is significantly increased, and with it, the information revolution devalues the power and wealth of industrial workers (that is, fewer people would work on the factory floor, in mines, on farms, on ships, and so on, and more people would be placed in offices with computers and processors — fewer "blue collars" and more "white collars"); large manufacturing companies would be compelled to diversify into information sectors; within companies, the value of the "knowledge worker" is increased at the expense of the value of industrial workers; the power and capabilities of management in large companies are enhanced; companies would be able to significantly increase the internationalization of information; and so on (STRANGE, 1988, p.131–133).

structure (STRANGE, 1988). According to her, for example, it is the number of nationals with access to higher education that differentiates States. The accumulation of education, information, and knowledge removes obstacles to access to credit (and not merely the accumulation of wealth in any form). And she further affirms that a shift in the transmission of power is taking place: gradually, power is moving from nations "rich in capital" to those "rich in information." For this reason, she considers that access to knowledge lies at the heart of social status and the distribution of power (Ibid., p.138).

2.6 Diffusion of Power

Having discussed relational power, structural power, and the primary structures defined by Strange (1988), it is now appropriate to present the phenomenon of the diffusion of power. This phenomenon is the subject of the work *The Retreat of the State: The Diffusion of Power in the World Economy*, from 1996. Although the expression "diffusion of power" appears in the title, it appears only once throughout the entire content of the work.[54] However, the term "diffusion" quite commonly appears associated with the word "authority."

According to Strange (1996), it is difficult to define authority. Explicitly, she does not define this concept in either of her two works. However, there are two distinct passages that elucidate its meaning. First, (1) in *States and Markets*, when discussing the broader use of the term "politics": "[...] Extending the definition of politics beyond states to all sources of authority, to all with power to allocate values, however, allows the two worlds of markets and states, of government and business, to be treated as one, rather than as two as in Gilpin's equation." (STRANGE, 1988, p.38, emphasis ours). And second, (2) in *The Retreat of the State*, when investigating how to identify who holds authority in the global political-economic arena: "[...] The first, basic question was 'Who, or what, is responsible for change?' The second was 'Who, or what, exercises authority — the power to alter outcomes and redefine options for others — in the world economy or world society?'." (STRANGE, 1996, p.184, emphasis ours).

In the first passage, authorities are those entities with sufficient power to allocate values in the social, political, and economic context. These values, according to Strange (1988), are those arising from human social organization: security, wealth, justice, and freedom of choice — considered by her as the four basic values of political economy (Ibid.,

[54]She uses the expression "diffusion of power" when discussing telecommunications companies. We highlight the following excerpt: "Yet in most societies, the political contest has always been between those who gave priority to the short-term advantages of financial and technological bargaining power and those who saw the longer-term advantages of social and political legitimacy as a result of their enlightened concern for the broader interests of civil society. In our own times, that contest continues — but this time on a global scale. Here, the diffusion of power among so many governments, and from them to non-state authorities makes it more difficult for policy-makers to take the long, more socially and economically enlightened view." (STRANGE, 1996, p.108–109).

p.5).

In the second passage, we can identify what authority means for Strange (1996). She makes clear that the authorities to which she refers are entities that have sufficient power to alter outcomes and define options for others — which is consistent with the first passage, but adds the relational aspect of influence over outcomes. By definition, therefore, within the analytical framework developed by IPE, the existence of authorities other than the State is presumed: the State is not the only entity with the power to allocate values, redefine options for others, or influence outcomes. The great test, however — that which determines whether an entity has authority (in fact, and not merely in potential) — is the outcomes (STRANGE, 1996, p.91). In other words, perceiving a non-state actor as an authority, within a given context, is an exercise in analyzing its influence over outcomes.

According to Strange (1996), in the political-economic landscape of the twentieth century, the power to allocate values and alter outcomes for others was essentially concentrated in the figure of the nation-state. The beginning of the concentration of authority in the nation-state started with the Treaty of Westphalia. Before that, a great deal of authority was concentrated in the Catholic Church.[55]

The diffusion of power is the inverse phenomenon: the power of the nation-state — both in allocating values and in exercising power over outcomes, from the analytical framework of IPE — diffuses throughout the social, political, and economic fabric to other authorities that at times rival the State and at times reinforce it.[56] In other words, "[...] The declining authority of states is reflected in a growing diffusion of authority to other institutions and associations, and to local and regional bodies, and in a growing asymmetry between the larger states with structural power and weaker ones without it." (Ibid., p.4). And, especially at the end of the twentieth century, the phenomenon of the diffusion of power emerged prominently: "[...] Authority over society and economy is

[55]According to her, "The Treaty of Westphalia of 1648 is familiar to all students of international relations as the benchmark of a new era in which the authority and sovereignty of the state would be unchallenged. By implication, it marked the virtual end of the constraints imposed on kings and princes by the Church." (STRANGE, 1996, p.125).

[56]The classification of these authorities occurs only in relation to the state actor itself. Strange (1996) suggests classifying existing authorities in relation to the authority of the State itself. In this way, let us imagine a continuous line on which, at one extreme, is placed the non-state authority that contests and challenges (or even threatens to replace) the authority of the State. And at the other extreme of this same line, the non-state authority that sustains and reinforces the authority of the State. In the middle of this line are placed authorities that exercise either reinforcement or rivalry in relation to state authority. Whether the authorities lean toward one end or the other of the line is determined by the State, since the perception of rivalry or reinforcement is made by the State itself. This perception is quite subjective and subject to change (STRANGE, 1996, p.92). From this, we suggest some examples: nightclub bouncers, professional street security guards, and private security companies are examples of authorities (formal yet non-supreme) within the security structure that sustain and reinforce the authority of the State by providing protection services to other actors (which may be individuals, groups of people, companies, properties, etc.). An example of rivalry, in this case, would be the so-called "parallel state," that is, organized criminal groups that offer protection and threaten violence against individuals, groups of people, companies, properties, and so on.

undergoing another period of diffusion after two or three centuries in which authority became increasingly centralised in the institution of the state." (Ibid., p.86–87).

Therefore, if we observe each of the primary structures that compose the analytical framework of IPE, we perceive that authority is shared with other actors. In sum, we can also identify the phenomenon of the diffusion of power, in synthesized form, in the hypothesis of the 1996 work, in which she states:

> My hypothesis, as explained in the last chapter, is that on many issues most states have lost control over some of the functions of authority and are either sharing them with other states or with other (non-state) authorities. The outcome in some cases is that no one is responsible for authority functions, even though they may pretend to be. It presumes some general decline in the power of most states and some gain in the authority of world markets and of enterprises operating in world markets. This shift away from states and towards markets is probably the biggest change in the international political economy to take place in the last half of the twentieth century. [...] I shall argue that one of the major shifts resulting from structural change has been the increased power and influence of the multinationals — more properly called transnational corporations (TNCs) — and the networks they set up and operate. (STRANGE, 1996, p.42–43)

The phenomenon of the diffusion of power presented by Strange (1996), according to her, explains political-economic movements that occurred in the second half of the twentieth century, such as the global scenario following the oil shocks and inflation. Traditional IR currents did not seek to explain this moment. In particular, the focus of her narrative concerns the U.S. economy. According to the British scholar, during this period, the American economy both grew and "spread" throughout the world, as did the sources of its power — which shifted from "land" and "people" to settle upon control over the structures of the global system.

In detail, Strange (1996) discusses the disorder caused by the inflations that followed the oil shocks from a global structural perspective — which in this case is the IS in which both state and non-state actors operate. There is recognition of the relevance of non-state actors, since they are imbued with structural power. However, the discipline of IR, and in particular the traditional theoretical currents within the field, cannot explain this same scenario because they commonly attribute to the State the unit of political analysis. It is this political perspective — that the State is the supreme actor in international politics — that collides with the economic perspective, since the latter acknowledges the relevance of non-state actors as subjects of analysis. For this reason, any IPE analysis must expand the unit of political analysis, for if the locus of power migrates from "land" and "people" to "control" over elements originating from the structures of the global system, the actor

in possession of this control is said to be an "authority" within this structure.[57] On the importance of admitting analyses of non-state actors, Strange (1996) argues that:

> Extending the focus of analysis from states to all forms of authority allows us to ask how, and by whom values are allocated and political decisions taken — in the wider sense outlined above — to affect outcomes. At one and the same time, we can ask about authority within states and outside them as well as just in their relations with each other. We can avoid the perennial temptation in the study of international relations to 'reify' the state, that is, to treat it as one 'thing', a unitary actor, as if France, say, or Japan, were a discrete personality. (STRANGE, 1996, p.37).

By extending the focus of analysis from the State to other forms of authority, IPE separates itself from the discipline of IR in its traditional sense. The adoption of a more encompassing definition of politics, which takes into consideration all forms of authority (including all those capable of allocating values), allows the union of Politics and Economics so that they may be treated as a single whole rather than as two separate areas.

2.7 The Three Dimensions of the Diffusion of Power

When Strange (1988, 1996) discussed structural power, primary structures, authorities, and the diffusion of power, she left an open invitation for others to explore the subject through reading, informed discussion, and disciplined thinking. In her 1988 work, she affirms that the book is not a conventional "textbook" because it would suggest ways of thinking about politics within the scope of the world economy. For this reason, we cannot call her interpretations a theory, but rather an analytical framework. On this point, she stated that:

> This is not a conventional textbook. Students are often given books to read which tell them what they are supposed to know, or else what they are supposed to think. This is not like that. It is going to suggest to you a way to think about the politics of the world economy, leaving it to you to choose what to think. [...] Before you there is not a set menu, not even an a la carte menu, but the ingredients for you to make your own choice of dish and recipe. This is partly because I believe profoundly that the function of higher education is to open minds, not to close them. The best teachers are not those who create

[57] But not necessarily the supreme authority: it may be the supreme authority (for example, Strange affirms that the State is the supreme authority in the security structure) or occupy a position below the supreme one (a mafia boss is an authority in the neighborhood where they reside when providing security to residents in exchange for their silence).

> in their own image a crowd of uncritical acolytes and followers, obediently parroting whatever they say or write. The best are those who stimulate and help people with less experience in and exposure to a subject than themselves to develop their own ideas and to work them out by means of wider reading, more informed discussion and more disciplined thinking. (STRANGE, 1988, p.9).

As a reader and student of Strange, her works stimulated me to think about the possibility of operationalizing the concept of diffusion of power. Moreover, I felt that there would be no inconsistency in seeking, within her literature, clues that could assist me in deepening my understanding of IPE and in attempting to operationalize the phenomenon — given that she herself, as a teacher and author, extends this invitation and encourages these activities. For this reason, after analyzing her text and reflecting on the conceptions she presented, I believe that the diffusion of power operates across three dimensions — which I have called "authority," "control," and "outcomes."[58] These three dimensions are grounded in Strange's own literature (1988, 1996), so that, in the process of operationalizing the phenomenon of diffusion, these three dimensions could be understood as "discrete qualitative variables" and, therefore, capable of receiving numerical values.

The next section of the chapter is organized as follows: (1) we seek to substantiate, from the literature, the reasons that lead us to believe that the diffusion of power operates across three dimensions — with emphasis on excerpts from the works that allow for this reflection; (2) to present the "valuations" of each dimension when translated into "variables" — that is, what values each of the three variables can receive and why.

2.7.1 The "Authority" Dimension

When the reader undertakes a careful reading of the two works by Strange mentioned in this dissertation, they have the capacity to observe that three elements are found very close to the core of the phenomenon of the diffusion of power — which, as is known, opened the way for analyses of the IS from the field of IPE. These three elements are authority, control, and outcomes.

Authority is a concept whose definition is quite complicated, as acknowledged by the British scholar herself. However, we can affirm that, in *The Retreat of the State*, in virtually all statements about the "diffusion of power," Strange used the term "diffusion of authority" — as if they were synonymous and interchangeable terms. Our interpretation is that they are not.

The term "authority" has, in our view, two interpretations that, despite being quite subtle, are sufficient to distinguish them: the use of the term "authority" sometimes

[58] These words are the respective translations of "authority," "control," and "outcomes" — words used by Strange in the context of her two works.

describes an entity that commands the trust of its peers and stakeholders (*being* an authority), and sometimes describes the exercise of power (*exercising* authority). We believe that the expression "diffusion of authority" (which Strange used in her work as nearly synonymous with "diffusion of power") is linked to the second interpretation, that is, the diffusion of the exercise of power (exercising authority). This is because if it referred to the diffusion of "being" an authority, this would translate into the "dismemberment" of the State, as an authority, into various other entities with lesser authority. In other words, the diffusion of authority, in this case, would mean the emergence of a plurality of lesser authorities, originating from the State and detached from it. And this is not what the phenomenon of the diffusion of power is about.[59]

Being an authority within the IS, viewed through the lens of the four primary structures, demonstrates that the actor has gathered sufficient authority to exercise it in a way that affects outcomes. We assume that this gathering of authority is granted by peers and stakeholders in two ways: via consent or subordination. An authority within the security structure is the State. Its peers (other States) and stakeholders (its nationals) formally grant it authority so that it may be recognized as sovereign in the IS, and thus flow the policies and agreements that derive from the recognition of sovereignty. Another authority within the security structure is the Italian mafia, illustrated by Strange (1996) through the organization "Cosa Nostra." This organization is recognized by its peers (other mafia groups) as an authority. Citizens who are directly affected by the activities of this organization (for example, inhabitants of a neighborhood with a high concentration of "Cosa Nostra" members) may not consent to the organization's authority (many do consent), but all subordinate themselves to this authority if they wish to avoid conflict. Both authorities, the "Italian government" and "Cosa Nostra," clash and conflict on the domestic stage because they rival each other. The Italian State views the mafia organization as a rival to its authority, and conflicts, grounded in the rule of law, ensue. In this example, what distinguishes the mafia organization's authority from the State's authority is formality. The Italian government is the authority that concentrates the identity of the Italian State through formal means — recognized through the democratic vote, to which the armed forces, other institutions, and citizens subordinate themselves. Similarly, the Italian national football team during a World Cup also concentrates, in the sporting domain, the identity of the State — but informally. The Italian mafia, on the other hand, is an informal and illegal authority.

Exercising authority is exercising power. This power is exercised directly through relational power and indirectly through structural power (STRANGE, 1996, p.91). In

[59]We have highlighted the passages in which Strange (1996) writes about "authority" and grouped them into two categories: passages that present authority as the exercise of power; and passages that present authority as an institution, as "being" an authority. These two groups can be found in the list of appendices. We recommend consulting "Appendix 1 — Being an Authority" and "Appendix 2 — Exercising Authority."

the example given above, both authorities — the Italian State and the mafia through the "Cosa Nostra" organization — exercise power because they influence outcomes for a set of individuals and institutions and redefine their options of choice. The Italian government is the supreme political authority within the territorial limits of the Italian State, which holds the legitimate use of force. The mafia, on the other hand, organizes itself through structures that exert influence over a set of activities and over the security of citizens, as they often act through coercion and violence.[60] While one is a formal authority, the other is an informal authority. But both exercise authority, both exercise power. One of the objectives of scholars in the field of IPE is "to try and untangle the complex web of overlapping, symbiotic or conflicting authority in any sector or on any who-gets-what issue." (Ibid., p.99).

Being an authority and exercising authority, although very similar, entail distinct yet complementary consequences. An actor can gather sufficient trust from its peers and stakeholders so as to be considered an authority on a given matter. This trust may have been granted through consent or through imposed subordination. In the first case, we can cite as an example an international organization whose members are States. At the outset, a group of States granted sufficient authority, through expressed consent, for the General Secretariat of this organization to begin its activities on a given matter. Over time, other States, observing the functioning of this organization, decided to participate as members. All of these member States are responsible for granting authority to the organization, which develops a series of binding agreements on the matter in which it specializes (in this case, it is recognized as an authority within the knowledge structure), which must be followed by all members.

Another way of gathering the trust of peers and stakeholders is through imposed subordination. Let us imagine what happens in the favelas dominated by drug trafficking in the city of Rio de Janeiro, Brazil. Distinct factions compete for power and shares of the drug market. Let us imagine that faction A holds authority over the hillside community and imposes a set of rules on the citizens who live there — such as identifying oneself every time one enters or leaves the neighborhood and not circulating after 10 p.m. Even though they do not consent to this set of rules imposed by the dominant group on the hill, without alternatives, the residents recognize faction A as an authority (in this case, within the security structure) and abide by its rules so that, in return, they do not face violence. In this scenario, faction B emerges, interested in dominating the hill and reaping profits from the drug trade. A "war" begins between the two groups, the consequence of which is the victory of faction B. The consequence of this is that faction B is now recognized as

[60]Strange (1996) highlights the suggestion of some sociologists regarding the origin of mafia authorities, stating that "Sociologists have argued that criminal gangs, like underground resistance movements in wartime or recalcitrant groups in prisons, tend to emerge when state authority, for whatever reason is already weakened, and the government has lost or failed to obtain the consent of the governed." (STRANGE, 1996, p.116).

the new authority on the hill. The residents of the neighborhood subordinate themselves to this new group.

In the first example, authority was recognized by the member States without the organization exercising power in a way that affected outcomes. In this first context, "being an authority" emerges before "exercising authority." In the second case, things change. Faction B "exercises authority," or rather, exercises power in a way that affected outcomes — it eliminated faction A and was recognized as the new authority on the hill. "Being" an authority and the exercise of authority are moments that complement each other — regardless of which moment came first. Exercising power reinforces the authority of the actor in question. However, it is important to emphasize that the actor tends to lose authority ("being an authority") when it is no longer capable of exercising power in a way that affects outcomes. This is at the heart of the issue raised by Strange (1996) when she stated that the authority of a non-state actor could only be determined on the basis of outcomes. It is of no use to be an authority without possessing the capacity to exercise that authority through power — over time, the trust of peers and stakeholders dilutes and the recognition as an authority on a given matter fades away.

Some further considerations are warranted regarding the recognition of authority through the trust generated by peers and stakeholders — specifically within the knowledge structure. Examples of this are expressed in Strange's literature (1988) in at least three instances. In Hindu society, religious authority was sustained by belief. This was capable of maintaining a set of rules over society regarding diverse activities that ranged from personal hygiene and marriage to the consumption of food through typical diets (STRANGE, 1988). The religious authority, represented by the "brahmins," therefore gathered the trust of peers and stakeholders such that segments of society voluntarily followed the precepts determined by the religious authority. It should be noted that this authority is located primarily within the knowledge structure.

On another occasion, speaking explicitly about the knowledge structure, Strange (1988) points out that authority and power are conferred upon those who "are acknowledged by society to be possessed of the 'right', desirable knowledge and engaged in the acquisition of it, and on those entrusted with its storage, and on those controlling in any way the channels by which knowledge, or information, is communicated." (Ibid., p.121). The recognition of authority within the knowledge structure — such as, for example, the authority of individuals who are part of the scientific community — is granted by society, which, to a certain extent, trusts that these members possess the knowledge they express. A researcher in the field of IPE, for example, holding a doctoral degree, is recognized by society as having knowledge on certain matters of this research agenda. The degree, conferred by an educational institution and recognized by a government body (representative of society in matters of education), is the granting of authority on the subject of IPE. It is from this granting, from this trust placed in them, that the researcher in this example

may enjoy a set of specific legal rights and prerogatives. It should be noted that, in this case, the authority is formal.

Finally, in a third instance, Strange (1988) comments on the trust of peers and stakeholders in the formation of authority within the scope of the World Administrative Radio Conference (WARC). In this case, she considers the hypothesis that the international bureaucracy responsible for WARC acted according to its own policies — that is, independently of state policy. She affirms that "[...] only if there is real evidence that the agency has some technical capability, or some special authority legitimated not by the approval of governments but by the consent and respect of those affected should it be considered separately from state policies." (STRANGE, 1988, p.233). Should this hypothesis be confirmed, it can be affirmed that the trust of stakeholders was a determining factor in the legitimation of this international bureaucracy's authority within the scope of the matters addressed by WARC.

These three examples are important for the discussion of this dissertation because they legitimize that authority, especially within the knowledge structure, is conferred through the trust of peers and stakeholders in the matter over which the authority claims to have knowledge. The perception of the degree of trust of peers and stakeholders — increasing trust, stable trust, decreasing trust — bears upon the "authority" variable present in the database generated for this research.

2.7.2 The "Control" Dimension

Like authority, /textitcontrol is also a highly relevant element for understanding the diffusion of power. We consider "control" to be one of the three dimensions of the diffusion of power. In *States and Markets*, Strange (1988) points to the role of control in the formation of power — with special emphasis on structural power, but also pointing to economic and political power, stating that:

> Banks, by controlling credit, have economic power. Equally, we can say that people have political power if they control the machinery of state or any other institution and can use it to compel obedience or conformity to their wishes and preferences from others. The trouble with this distinction, however, is that when it comes to particular situations — particularly in the international political economy — it is very difficult (as some later examples will show) to draw a clear distinction between political and economic power. (STRANGE, 1988, p.25)

Here we can perceive that control over an object relevant to the achievement of desired outcomes lies at the core of economic and political power. In the case of banks, the object is credit, for it is control over it that allows banks to have sufficient power to influence

outcomes in the economic arena.[61] Equally, control over the state apparatus by a political group, for example, confers upon it sufficient power to influence outcomes in the political arena — at least to a certain extent.

Similarly, we examine the relevance of control in the context of the four structures from the following quotation by Strange (1988) on the sources of structural power:

> These four, interacting structures are not peculiar to the world system, or the global political economy, as you may prefer to call it. The sources of superior structural power are the same in very small human groups, like a family or a remote village community, as they are in the world at large. The four sources, corresponding to the four sides of the transparent pyramid, are: control over security; control over production; control over credit; and control over knowledge, beliefs and ideas. Thus, structural power lies with those in a position to exercise control over (i.e. to threaten or to preserve) people's security, especially from violence. It lies also with those able to decide and control the manner or mode of production of goods and services for survival. Thirdly, it lies — at least in all advanced economies, whether state-capitalist, private-capitalist or a mix of both — with those able to control the supply and distribution of credit. Such control of credit is important because, through it, purchasing power can be acquired without either working for it or trading for it, but it is acquired in the last resort on the basis of reputation on the borrower's side and confidence on the lender's. Fourthly and lastly, structural power can also be exercised by those who possess knowledge, who can wholly or partially limit or decide the terms of access to it. (STRANGE, 1988, p.26, emphasis ours).

In other words, the source of structural power resides in the control of objects originating from the primary structures. In this regard, our attention turns especially to the knowledge structure and the role that control plays in the formulation of power originating from it. Here, it bears recalling once more that the power originating from this structure is also conditioned by control over the channels through which information circulates and is stored (STRANGE, 1988). Let us consider an example of this dynamic.

We can imagine an institution dedicated to research on marine animals. All the knowledge produced through research, data collection, and sample analysis rests upon prior knowledge on a given subject. Upon inferring that the whale is a mammal and not a fish, the researcher can devote themselves to analyses of problems typical of mammals,

[61] Another example, to illustrate the role of control in power, refers to Great Britain's political control over India. This political control allowed London to extract gold annually and thus use control over the gold supply to influence the Pound-Rupee exchange rate and other instruments of exchange rate policy. British capital flows were essential for the maintenance of economic growth in the pre-1914 world (STRANGE, 1988, p.101).

such as the development of milk in this specific species of whale, for example. But they can only do so if they know that the animal is a mammal and that mammals possess mammary glands. Someone, at some prior moment, produced the knowledge that whales are mammals that inhabit the oceans. This information was stored so that, from it, new studies followed in succession. Furthermore, this knowledge was communicated and shared among various members of the scientific community.

Now let us imagine that, by terrible fate, a great catastrophe befell a large part of human knowledge about animals of all species, and that this institution dedicated to research on marine animals, along with a handful of scientists, was one of the few to be spared from this terrible fate. Let us also imagine that all the knowledge produced and stored by this institution resides in the "cloud" — that is, in some abstract storage location on a computer server. In this hypothetical scenario, the senior researcher of this institution and the IT professional hold great authority and structural power because they control access to the information channels — the researcher by virtue of having experience and knowledge recognized by peers; and the IT professional by providing access to the storage of this knowledge through the channels where information circulates and is stored, that is, in the cloud and in the digital computer network. Both are important for the society that carries on after the catastrophe. Equally, other individuals and entities (such as the hypothetical institution) in this scenario may have the capacity to gather sufficient authority on a given matter due to the knowledge they possess — such as, for example, knowledge of survival in nature. For, as Strange (1988) said, "a knowledge structure determines what knowledge is discovered, how it is stored, and who communicates it by which means to whom and on what terms." (STRANGE, 1988, p.121). From this, we can infer that those who control objects (1) determinant for the type of knowledge that will be researched/discovered, (2) of the type that store information, (3) that form communication channels through which knowledge is transferred — these are relevant objects within the knowledge structure and confer upon those in possession of their control with power. For, "[...] Knowledge is power and whoever is able to develop or acquire and to deny the access of others to a kind of knowledge respected and sought by others; and whoever can control the channels by which it is communicated to those given access to it, will exercise a very special kind of structural power." (STRANGE, 1988, p.30)

Some examples of entities that, to some extent, controlled objects considered important within the knowledge structure and ascended to power are highlighted in Strange's literature (1996): the Catholic Church in medieval Christian Europe; the scientificist State during World War II; companies that hold a monopoly over a specific technology; among other cases.[62] Control over a given object represents power — which, naturally,

[62]We have compiled in a table examples from both of Strange's works (1988, 1996) that refer to "control" and the "object" of control. It is possible to verify that in some instances she points out that "control" represents power. See "Appendix 3 — Control, 1988" and "Appendix 4 — Control, 1996."

influences outcomes. For this reason, control is one of the dimensions of the diffusion of power.

2.7.3 The "Outcomes" Dimension

Outcomes constitute the third dimension of the diffusion of power. This dimension is intimately related to the dimensions of authority and control because it represents the existence of the effectiveness of both. We may assume that a given actor, in the context of IPE, holds authority over a matter. Through this authority, obedience and subordination are conferred upon them. We may also assume that this actor holds control over an object considered relevant, by peers and stakeholders, in the political-economic arena. Consequently, this actor is considered important within the context of IPE. In both situations, what attests to the actor's authority, and what attests that it holds control over the object, is its capacity to influence outcomes. That is, if it is verified, through the outcomes, that the actor had the capacity to influence the status quo, its authority is reinforced and/or its control is confirmed. If its capacity to influence outcomes is not verified, its authority is shaken — which means that the trust of peers and stakeholders will be diminished — and/or control over a given object will be questioned. The "outcomes" dimension is the one that confirms, questions, or rejects the effectiveness of the power held by the actor in question. It should be emphasized that power bears upon outcomes, through the status quo, in two ways: maintaining it or altering it.

The emergence of information networks based on microelectronics, of which the global computer network is a part, gave rise to the cyber domain. The "outcomes" dimension is concerned with the incidence of power upon the status quo in the real plane, and not in the digital plane. That is, it is the outcomes that bear upon the real, geographical plane that are considered relevant for the analysis of the diffusion of power, because it is in this plane that the actors are found. Outcomes that bear only upon the digital plane, with no incidence upon the real, exist in a closed system of abstraction and, for this reason, are not relevant for the analysis of the diffusion of power according to the field of IPE. The "outcomes" dimension therefore has, as its principal content, the effect on the geographical reality where the actors are found. Outcomes generated in the cyber plane will be taken into consideration only if they also bear upon geographical reality. In the introduction, we pointed to the example of an individual participating in a virtual game for personal leisure and in the context of a championship.

2.7.4 Operationalization of the Dimensions

The three dimensions mentioned above were operationalized so as to become discrete qualitative variables. Each of the three variables receives values that vary according to the dimension, as explained in the introduction of this dissertation.

The first variable, authority, has as its content the sense of trust. This sense concerns the trust that peers and stakeholders in the matter place in the authority in question. The trust deposited (or the lack thereof) designates growth, maintenance, or decline of the actor's level of authority over a given matter. For this reason, this variable can receive the integer values "−1" (decline), "0" (maintenance), and "+1" (growth).

The conceptions of "growth," "maintenance," and "decline" were drawn from Strange's own literature (1988, 1996). In *States and Markets*, she discussed this gradual variation of authority. We highlight some examples, such as when she writes about the decline of the authority of the Catholic Church in medieval Christian Europe:

> The cultural and social unity provided by the Church created a primitive kind of common market in Europe. It also made possible the accumulation of capital — especially by the great religious orders. As the Church's authority declined, the emerging nation-states inherited from it an economy already pregnant with the growing points of technical change and a commercial structure ready for exploitation by a nascent merchant class. (STRANGE, 1988, p.71–72)

At another point, it is understood that the decline of the Catholic Church's authority within the knowledge structure — that is, with regard to the knowledge produced, stored, and shared in society — was gradually replaced by the growing authority of the scientific State. While the Church saw its power diminish, the scientific State saw its power over society and its activities grow:

> [...] It [the Treaty of Westphalia] marked the virtual end of the constraints imposed on kings and princes by the Church. [...] To the same end, the state took over from the Church responsibility for enlarging the education system, in universities as in schools. New patent laws secured monopoly rights for technical innovation through the institution of intellectual property rights. [...] The new technology was also made to serve the interests of the state and to reinforce its power. Even though the technologies of telegraph, railroad and radio were initially developed to serve the interests of business and finance, the cumulative consequence of all three was to tighten the grip of government over the individual. [...] Aided by differences of language, national governments could use technology to keep control by censorship, by monopoly or by restrictive licensing over national systems of education, over national newspapers and broadcasting and even over the publication of books and periodicals. Thus, in this new knowledge structure, the authority of the Church was displaced by the extended authority of the scientific state. [...] In the change, however gradual or slow, from the knowledge structure dominated

> by the Church to the knowledge structure dominated by the scientific state, there were certain politically crucial changes. (STRANGE, 1988, p.125–127)

After dominating the knowledge structure and legitimizing itself as the supreme authority within the knowledge structure, the scientific State "fought" for the maintenance of its level of authority — as we can see in this passage highlighted by Strange (1988):

> But, once established, the authority of the state, legitimated by the knowledge structure, strove hard to maintain its monopoly position. The more its authority was threatened the more vigorously it was defended. The state, in many cases, asserted a unique right to judge what was acceptable and unacceptable conduct. The Church had asserted its legitimate authority to decide what constituted a 'state of grace' rather more than what constituted good conduct. The scientific state asserted its legitimate authority, derived from popular loyalty to and belief in the concept of the nation, to decide what was good conduct, who was loyal or disloyal, what constituted dissidence or treason to the state. (STRANGE, 1988, p.128, emphasis ours).

On another occasion, Strange (1988) explains both the decline of the U.S. government's authority over U.S.-based transnational corporations and its growth over foreign transnational corporations operating on American territory:

> Washington may have lost some of its authority over the US-based transnationals, but their managers still carry US passports, can be sub-poenaed by US courts, and in war or national emergency would obey Washington first. Meanwhile, the US government has gained new authority over a great many foreign corporations operating inside the United States. All of them are acutely aware that the US market is the biggest prize in the competitive game. My guess, from talking to corporate executives — American and European — is that on balance US authority in the world economy has actually increased, not declined. (STRANGE, 1988, p.239).

In *The Retreat of the State*, 1996, in which she discusses the diffusion of power proper, her central argument concerns the decline in the quality of the authority of the governments of most territorial States — and not the decline in the quantity of the exercise of authority (STRANGE, 1996). In any case, her central thesis rests upon the diminution of the authority of States over people and activities within their territories, not the replacement of the State's authority by other non-state authorities. The existence of other non-state authorities at times competes with, at times rivals, the state authority across the four primary structures defined by Susan Strange's IPE.

When discussing the rivalry between the authorities of the Italian State and the mafia organization "Cosa Nostra," Strange (1996) points out that the relationship between them became unstable on two occasions: either when the authority of either party weakened, or when the authority of one of the parties became strong enough to threaten the other. She stated that:

> Such arrangements worked (for a time at least) always provided both sides respected — and made their subjects respect — the implicit bargain regarding the division of responsibility. They became unstable however when the authority of either party was weakened, or when the non-state authority became so strong that it was thought to threaten the state. (STRANGE, 1996, p.119, emphasis ours)

Finally, she reinforces the idea of increase, maintenance, and decline of authority when discussing the role of certain professions in the global political economy landscape, such as insurance business managers:

> Another consequence is to give added authority to the insurers. As technological and financial change affects their business, they respond by putting a higher price on premiums for some risks over others, or by refusing to offer insurance cover on any terms whatsoever. [...] They can, and indeed do, exercise the same kind of arbitrary authority over others when they refuse, for example, to sell insurance against theft to houseowners unwise — or unlucky — enough to live in burglary prone streets. Or, when they deny marine insurance to shipowners whose masters take the ship into a war-zone, as happened during the Iraq war. [...] For if, as I have argued, authority in political economy is recognisable by the power to alter or modify the behaviour of others by using incentives and disincentives to affect the choice and range of options, there can be little doubt that as the world economy grows, the costs and risks of economic transactions escalate, allowing insurers and reinsurers to exercise increasing authority in and over the system. (STRANGE, 1996, p.133)

Given that Strange (1988, 1996), on various occasions, discussed authority and fluctuations of authority, we believe that "growth," "maintenance," and "decline" of authority bear upon the balance of power.[63] The "authority" variable represents one of the dimensions of the diffusion of power.

The second variable, control, has as its content the sense of exercise or operation of a given object by an actor. Control over objects can be absolute, partial, or none. It is

[63]The balance of power is understood here as the interplay of forces, of power among state and non-state actors in the IS. It should not be understood in the classical sense of the expression as used in Realism.

absolute when the actor in question is solely responsible for the control of a given object, directing it as they see fit. It is partial when they are not solely responsible for controlling the object, or when they depend on other actors to control the object. And there is no control when they are not responsible for controlling the object, or when they have no access to the object.

A classic example of the role of control in Strange's literature (1988) concerns the power that bureaucracy has over the object produced by producers and consumed by consumers — which directly affects the production and the economy of a domestic market, for example. She stated that:

> Even in a command economy, there is, behind the veil of bureaucratic control, a kind of bargain between authority in the form of state ministries, and market in the form of consumers and producers. To maintain the authority of the state, a bargain has to be struck with the producers — managers and workers — to reward them sufficiently and to give effective enough incentives for them to produce the goods and services that will sell to consumers. (STRANGE, 1988, p.39–40)

The incentives that the State provides to producers, so that they produce a sufficient quantity to meet the consumer market, must be such that the absence of the product does not bear upon the economy, for, after all, the producers have absolute control over the product — not the State. The latter, indirectly, makes use of incentives to bear upon production. Its control over the product is partial.

Another example discusses multinational companies that suffer appropriation by the State. Although these companies are compensated, as mandated by international law, the State often faces frustrations: in such cases, the States hold the production, the machinery, the resources to exploit the market, but not the technology, knowledge, and market access. After all, market access remains under the control of the former dispossessed companies. It is they who hold control over technology, knowledge, and market access. And this control means power. In particular, Strange (1988) cites the cases of Nigeria and Chile, stating that these countries:

> They began by nationalizing them, first the mineral and oil companies and then banks, insurance, breweries and other enterprises. Their right to do so — since industrialized countries had often done the same — was unchallenged provided only that they observed the rule of customary international law that compensation should be made promptly, in full and equitably. Yet the developing country governments very often found that they had won an empty victory, and too often at a high price. They had the mines, or the oil wells, but not the same power to exploit the market. Whether it was Chilean copper

> or the Guinness brewery in Nigeria, the displaced companies kept control over market access, by making long-term contracts with the customers, for instance. They also had command of the technology necessary to remain competitive in world markets. (STRANGE, 1988, p.85, emphasis ours)

In the case of the knowledge structure, the Catholic Church had its power and authority reinforced by control over the means of communication (sacred books, literacy in the Latin language — official within religious rites) (STRANGE, 1988). For Strange (1988), it is control over access to knowledge that enabled the maintenance of power within the Catholic Church — which indicates that rival authorities within this structure had to be eliminated or discredited (STRANGE, 1988, p.124). The Catholic Church's control in medieval Christian Europe over knowledge was, at times, absolute. The weakening of the Church's authority within the knowledge structure, in the face of the growing authority of the scientific State, brought to the fore the relevance of science and the scientific community. The axis of supreme authority within the knowledge structure shifted from the Church to the State. The sacred scriptures and the Latin language were replaced by scientism and the English language. The belief, on the part of peers and stakeholders (society in general and national governments, principally), in Science (and in the scientific community, consequently) as an authority over natural facts signified the erosion of the Church's authority over the same matter — relegating it to questions of spirituality and human faith (STRANGE, 1988). In this context, the Church's control over the means of communication did not retain the same relevance: postal services, telegraphs, and the telephone — originating from discoveries by the scientific community and controlled by States and private companies — meant power for those who held their control. In other words, the objects relevant for the achievement of desired outcomes within the knowledge structure changed, and they meant power for whoever held control over these new objects.

On another occasion, Strange (1996) cites the monopoly of control by companies over a technology, supply, marketing system, or even a brand. In the global market, this monopoly means power over the set of activities of the sector and consumers interested in the specific products of this company. Over time, it may be that the technology becomes shared (reverse engineering is one of the most commonly used tools) and the power that derives from control is, little by little, eroded — until a new technology is developed and monopoly over it is established. Or, as in the case of cartels that control the world's supply of diamonds: their power derives from the tight, nearly absolute, control over supplies. According to Strange:

> [...] She admits that the most effective cartel of the four she studied, that in diamonds, almost entirely owed its success to the tight control over supplies

> exercised by one firm, Anglo-American, and the majority owners, the Oppenheimer family. The supporting role of the South African, Soviet and Israeli governments was just that — supportive. (STRANGE, 1996, p.149).

There are other examples of control over an object, whether total, partial, or none. We suggest consulting "Appendix 3 — Control, 1988" and "Appendix 4 — Control, 1996."

Finally, regarding the "outcomes" variable. There are only two types of outcomes: those that alter the status quo; and those that do not. The alteration of the status quo (of the current state of affairs, or rather, the present state of something) signifies a change of state. Altering the status quo entails the replacement of one situation by another. The non-alteration of the status quo, in turn, entails its permanence, its reinforcement. In other words, there is a contest between forces for the alteration or permanence of the status quo. There is no alternative beyond these two. It should merely be recalled that the status quo refers to the region where the actors are found, that is, the real, geographical plane (and not the abstraction of information systems such as the cyber domain).

2.8 Power in the Cyber Domain

In this section, we offer brief considerations on power in the cyber domain drawing on two leading figures in the field of International Relations: Susan Strange and Joseph Nye Jr.

First, and above all, it must be established that the two works by Strange used in this research, *States and Markets*, 1988, and *The Retreat of the State*, 1996, do not point to indications of IPE in the specific context of the Internet. In 1988, the Internet had not yet been commercialized.[64] In 1996, a small portion of the world's population was taking its first steps on the global computer network. Studies on phenomena originating from the new cyber domain were few. However, even though she did not specifically discuss IPE in the context of the global computer network, Strange elucidates interesting points of discussion regarding technological changes and information systems from the perspective of the knowledge structure. We highlight some points that we believe will be capable of providing sufficient grounds for considering the study of IPE in the cyber domain—the essence of the present research.

Second, we chose to present some of the recent studies by Joseph Nye on account of his cybernetic considerations and because he discusses "diffusion of power" and "power transition" in his work—even though his discussion of "diffusion of power" is not related to the discussion that Strange conducts. Nye is perhaps the greatest exponent in the field of IR to have offered considerations on the discipline in the cyber domain.

[64] According to Ceruzzi (2003, p.321), the Internet was commercialized in the United States in 1995.

2.8.1 Susan Strange: Technological Innovations, Information Systems, and the Diffusion of Power in the Knowledge Structure

In the work *The Retreat of the State*, Strange (1996) argues that general propositions about authority in the context of IPE were being developed at the end of the twentieth century. One of these propositions stated that the authority of the governments of all States had weakened as a result of technological and financial changes and the accelerated integration of national economies into a single global market economy. For us, it is relevant to point out the role of technology in this end-of-century scenario which, according to her, is largely neglected by academia—even though it is of extreme importance for the consolidation of this new dynamic. On this matter, Strange states that

> The argument in the book depends a good deal on the accelerating pace of technological change as a prime cause of the shift in the state-market balance of power. Since social scientists are, not, by definition, natural scientists, they have a strong tendency to overlook the importance of technology which rests, ultimately, on advances in physics, in chemistry and related sciences like nuclear physics or industrial chemistry. [...] This simple, everyday, commonsense fact of modern life is important because it goes a long way to explaining both political and economic change. It illuminates the changes both in the power of states and in the power of markets. Its dynamism, in fact, is basic to my argument, because it is a continuing factor, not a once-for-all change. For the sake of clarity, consider first the military aspects of technical change, and the civilian aspects – although in reality each spills over into the other. (STRANGE, 1996, p.7–8)

Strange, in addition to recognizing the technological factor as an essential cause of shifts in the balance of power, indicates that it is the element capable of explaining both economic and political changes. And the new information technologies—stemming from specific knowledge and discoveries—represented to a large extent by the Internet, bear great responsibility in this regard. The knowledge necessary for the creation of these new systems conferred authority upon specific groups of scientists within the knowledge structure. Likewise, the other structures (security, production, and finance) had, to a lesser or greater degree, an incidence upon the development of the Internet.

From the perspective of the security structure, we can perceive the concern of military sectors of the U.S. armed forces in creating a communication system capable of withstanding nuclear attacks. From the production structure, computer component manufacturers had to reach a consensus regarding the design and technologies implemented in hardware so as to "allow" the standardization of access to the global network. The harmonization

of the production of machines and components enabled the mass purchase of computers capable of meeting the hardware and software prerequisites for connecting to the Internet. From the finance structure, we observe that the commercial opening of the Internet boosted the software and digital platform industry, capable of moving the financial market and gaining authority in the computing sector.[65]

In sum, the Internet is the product of three complementary forces in the second half of the twentieth century—Big Science,[66] the military, and the scientific community.[67] At the end of this century, States, companies, and part of the civilian population gained access to the commercial Internet and entered the cyber domain. If it is true that geographical boundaries no longer coincide with the extent of political authority over the economy and society, as Strange (1996) affirms, it is reasonable to suppose that this authority seeks to legitimize itself within the domain of cyberspace—where communications flow, service exchanges take place, and new software technologies originating from knowledge are born—after all, "the network society" is a new dimension of society itself.[68]

It should be recalled that the Internet is a hybrid regime composed of physical and digital aspects (LIBICKI, 2009). It operates through a web of telecommunications infrastructure that is truly distributed across the globe (CANABARRO, 2014, p.26). Beyond the physical structure of cables, satellites, modems, routers, etc., it responds to a digital structure, where protocols, addressing, packet routing, software, etc., are found. According to Canabarro (2014), "the Digital Era concerns basically the manipulation, storage,

[65]Information regarding the origin of the Internet is discussed in more detail in chapter 2 of this dissertation.

[66]For Schatz (2014), "Big Science" was not the result of specific events such as the "Manhattan Project" or the "Apollo Programme," but developed gradually from "Little Science." For Hallonsten (2014), one of the manifestations of the relationship between science and the State is "Big Science," which lies at the axis between fundamental science and military research and development.

[67]According to Castells (2001, p.17), the Internet was a discovery stemming from the intersection of Big Science, military research, and the culture of freedom. The first was developed by the Americans throughout the twentieth century; the second is evidence that the military sector is also a driving force behind technological innovations stemming from its own research and development; and the third demonstrates the participation of the civil sector through university academics who stimulated the growth of the global network. On this topic, the studies by Castells (2005) are relevant. For the author, the world is undergoing a multidimensional structural transformation associated with the emergence of a new technological paradigm. This emerging society, characterized as an information society or knowledge society, differs from previous societies in that it is "based on microelectronics, through technological networks that provide new capabilities to an old form of social organization: networks." (Ibid., p.17). In this sense, the author considers that the new "network society" is empowered by the most "extraordinary technological revolution of humanity, one capable of transforming our communication capacities, that allows the alteration of our codes of life, that provides us with tools to truly control our own conditions, with all its destructive potential and all the implications of its creative capacity. [...] What we know is that this technological paradigm has performance capabilities superior to those of previous technological systems." (Ibid., p.19). Thus, it is concluded that "network communication transcends borders, the network society is global, it is based on global networks. So its logic reaches countries all over the planet and diffuses through the power integrated into global networks of capital, goods, services, communication, information, science, and technology." (Ibid., p.18)

[68]On this matter, the studies by Castells (2005) are relevant. For the author, the world is undergoing a multidimensional structural transformation associated with the emergence of a new technological paradigm.

and propagation of information in digital format through electronic devices, which allowed the development of digital computing." (CANABARRO, 2014, p.26). The point is that when discussing the development of the Internet, one discusses both the physical aspect and the abstract aspect of the ideas that drive digital and technological innovations. The knowledge structure contributed to a large extent to the creation of the Internet. All of this provides evidence for the existence of structural power in this new technological paradigm. We emphasize that Strange herself (1988) pointed out, at the end of the 1980s, that States were aware of the importance of intangible resources that originate from a strong civil society. For them, these intangible resources could even compensate for deficiencies of the nation such as population size, territory, or military force.[69]

Another important point is that Strange (1988) gave indications of what would be considered important knowledge for the knowledge structure. This knowledge should deal, especially, with (1) any change in the supply, or control, of information and the systems that encompass communication in general; (2) changes that could bear upon the use of language or non-verbal channels of communication; (3) and also changes in perception considered fundamental regarding the human condition that could influence value judgments. Through these indications, we can consider that the Internet is a relevant landmark within the knowledge structure.

Although she did not write about the Internet, at the end of the 1980s Strange demonstrated awareness of the technological changes underway in society, having highlighted in her work two technical innovations that she considered especially central to the debate that was taking place in that period. The first innovation referred to the development of sophisticated computers; and the second innovation concerned electronic communications via satellites. These two innovations, according to her, were responsible for immediate results: they unified national markets across all products and services (STRANGE, 1988). These statements about technological innovations are relevant because they demonstrate that, even though she did not discuss the Internet, Strange was not "asleep" regarding the events unfolding at the end of the 1980s and 1990s that culminated in the rise of the global computer network. Her analytical effort regarding information systems and technological innovations in computing, although brief, resided essentially within the knowledge structure. And she considered the existence of developments originating from the knowledge structure to be exceedingly important for IPE—since competition among States at that time could be read as competition for technological leadership.[70] On this matter, she stated that

> The first of these developments is that the competition between states is be-

[69]Some States also include in this domain control over communication systems, air and maritime transport systems, and command of technical skills, for example (Ibid., p.38).

[70]Although the results or conclusions of these developments were not clear in her time, she argued that there was sufficient evidence to support this assertion (STRANGE, 1988, p.136).

> coming a competition for leadership in the knowledge structure. [...] Today, the competition is for a place at the "leading edge" (as the jargon has it) of advanced technology. [...] This is something that most ordinary people are already aware of and that is already well reflected in much popular fiction, in films and books. But it is something that has still be fully absorbed by many theorists, both in international relations and international economics. This radical change will require an equally radical revision of realist assumptions about the nature of international relations. [...] The second development resulting from change in the knowledge structure is that of the increasing asymmetry between states as political authorities in the acquisition of knowledge and access to it. [...] Although American universities and American corporate research centres may be challenged in certain rather narrow fields of advanced technology, their dominance over the broad range is still uncontested. [...] Thirdly, change in the knowledge structure is bringing about new distributions of power, social status and influence within societies and across state boundaries. [...] Power is passing to the 'information-rich' instead of the 'capital-rich'. (STRANGE, 1988, p.136–138)

At the end of the 1980s, the author perceives the technological transformations and their political impact within the knowledge structure—strong enough to highlight the importance of analyses through the field of IPE. The transformations stemming from the transition of the network society to a microelectronic base, as mentioned by Castells and Cardoso (2005), combined with other technological changes in diverse sectors, seem to lead Strange to conclude that this is indeed the structure undergoing the most rapid changes, even though it is the most neglected primary structure (STRANGE, 1988). It is in this context that she emphasizes that the concerns of IPE scholars must turn to the nature of power exercised through the knowledge structure; and to the centers of power—questioning whether these centers are undergoing significant changes (STRANGE, 1988, p.136).

Based on what has been discussed so far, everything indicates that there are no reasons to disregard the analysis of IPE in the context of the Internet—since it is a space where products and services are commercialized, agents exchange information and share knowledge, new abstract technologies are developed and implemented as new non-verbal communication systems. In sum, if it is true that IPE studies political and economic developments in a complementary manner, thus accompanying society, there is no reason to suppose that it should not be present in the new dimension of society: that which is grounded in networks and based on the microelectronic foundation—cyberspace.

2.8.2 Joseph Nye Jr.: Cyberpower, Diffusion, and Power Transition

The American Joseph Nye Jr. is known, especially, for his formulations on Soft Power and Hard Power. In 2011, he published the work *The Future of Power*, in which he describes the newest modality of power in the twenty-first century: Cyberpower. A year earlier, Nye had already stated that "cyberspace is a new and important domain of power." (NYE, 2010, p.2). He also defined Cyberpower:

> Cyberpower can be defined in terms of a set of resources that relate to the creation, control, and communication of electronic and computer-based information – infrastructure, networks, software, human skills. This includes not only the Internet of networked computers, but also Intranets, cellular technologies, and space-based communications. Defined behaviorally, cyberpower is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyberdomain. Cyberpower can be used to produce preferred outcomes within cyberspace, or it can use cyberinstruments to produce preferred outcomes in other domains outside cyberspace. (NYE, 2011, p.123)

Nye acknowledges that Cyberpower is also related to a set of resources. These resources are not tangible, as they are related to the creation, control, and communication of information based in the dimension of electronics and computers. That is, Cyberpower, described by Nye (2011) as representative of the power proper to the twenty-first century, appears to correspond to the type of structural power originating primarily from the knowledge structure of Susan Strange (1988)—with the sole difference of being a type of power existing exclusively in the domain of cyberspace.

We can correlate the passage highlighted above with Strange's works on structural power and the diffusion of power. In this sense, we identify the duality of Cyberpower: just as the power exercised in the IS according to the field of IPE, it also appears to be associated with both relational and structural power. Directly, Cyberpower is exercised through relational power—as it reflects the abilities to obtain desired outcomes. Indirectly, Cyberpower is exercised through structural power because its core is grounded in the set of resources related to the creation, control, and communication of information—or rather, knowledge. Just as Strange (1988), who observes power in the IS from these two perspectives, Nye's Cyberpower (2011) also exhibits this duality.

It is interesting to note how Nye (2011) acknowledges that cyberspace is indeed a new domain of power—one that begins at the end of the twentieth century. According to him, by virtue of being a domain in itself, this new arena requires the special attention of intellectuals and IR scholars, if they wish to understand the landscape of international

politics in the twenty-first century in a more comprehensive manner. This attention is necessary because, according to him, "Such cyber transformations are still fanciful, but a new information revolution is changing the nature of power and increasing its diffusion." (NYE, 2010, p.1). As can be observed, Nye (2011) also discusses the diffusion of power. However, unlike Strange (1996), he does not use the context of the primary structures to ground the phenomenon of the diffusion of power in cyberspace.

In the work *The Future of Power*, Nye (2011) acknowledges that two types of power shifts are occurring in the twenty-first century: power transition and power diffusion. In the first case, power transition refers to the displacement of power in a horizontal direction—that is, from one dominant State to another State. This process is considered familiar by the IR literature and is evidenced by studies of History. In the case of the new millennium, it refers especially to the displacement of the axis of power from the West to the East (NYE, 2011). Power diffusion, according to him, would be a new and recent process that designates a displacement of power in a vertical direction—which grounds the relevance of new (non-state) actors in the IS.

According to him, when it comes to cyberspace, one observes that one of the factors contributing to the diffusion of power is that a portion of the activities occurring in this domain are beyond the reach of the State. Or rather, beyond its control (NYE, 2011). The emergence of new actors, combined with the State's lack of control, promotes the diffusion of power in cyberspace. This massive emergence of a myriad of actors becomes possible through the reduction in the cost of information transmission. Technology rapidly loses its cost value. The new actors in the cyber domain, according to him, compete for power and challenge the State. It is for this reason that Nye (2011) believes that network centrality is the key dimension of power in the twenty-first century.[71]

But in what way does the rise of various actors on the global computer network contribute to the diffusion of power? In the following manner: the sharp increase in the number of users with access to the global network is explained by the reduction in the cost of entry to cyberspace. This new domain has inherent characteristics that are capable of promoting what Nye calls the "reduction of power differentials" (NYE, 2011, p.150). The reasoning is relatively simple: the domain of cyberspace is extremely new when compared to the domains of land, sea, and air. And in these domains, not all "pieces" possess "sufficient cards" to begin the game of power. Cyberspace, contrary

[71]If we correlate this with the studies led by Strange (1988, 1996), we could affirm that the actors capable of competing for power in this new domain represent authorities in the knowledge structure. Their abilities in the cyber domain at times rival and challenge the power of the State (in maintaining activities and individuals subordinated to its authority), and at times reinforce the power of the State when allying with it. Here, it is worth remembering that the development of software technologies is not confined to computing universities or technology sector companies. Any individual with access to the Internet, and sufficient knowledge, can develop computer programs, applications, and software that will be used by other actors on the network or outside it. We consider this to be strong evidence of the knowledge structure in the domain of cyberspace.

to these domains, and due to its reduced cost of access, enables the entry of different "pieces" with "sufficient cards" to begin the game of power. Nye even presents some targets of power in the domain of cyberspace—see "Appendix 2 — Physical and Virtual Dimensions of Cyberpower."

In summary, we can say that the low cost of entry to cyberspace—which characterizes the emergence of new actors—combined with the inherent characteristics of this domain, are responsible for promoting the reduction of power differentials among actors. In the cyber domain, power among different actors tends to equalize. After all, "Distributed Denial of Service Attacks"—known as "DDoS" attacks—an instrument of power in this area, for example, can be launched by any individual on the network—States, companies, individuals, organizations, etc., as long as they possess the knowledge. Different actors possess different power resources in cyberspace. The gap separating state and non-state actors narrows in many instances. This narrowing is the distinguishing feature of this new domain[72] (NYE, 2011).

Finally, two observations. First, for Nye (2011), power diffusion and power equalization are not the same phenomenon. Second, Nye (2011) recognizes that "although cyberspace may create some power shifts among states by opening limited opportunities for leapfrogging by small states using asymmetrical warfare, it is unlikely to be a game changer in the power transitions [...]." (NYE, 2011, p.151).

The changes in information systems and recent innovations in the field of computing were pointed out by Strange (1988) as relevant and deserving of analysis by IPE—still in the 1980s. More than 20 years later, Nye (2011) points out that the diffusion of power in cyberspace demonstrates that the new cyber domain is a key dimension for understanding power within the discipline of IR in the twenty-first century.

2.9 Conclusion

The objective of this initial chapter was to present the theoretical framework adopted by this research: IPE as developed by the British scholar Susan Strange. In particular, we are interested in the theoretical discussion surrounding the phenomenon of "diffusion of power"—given that this research seeks to understand how, and to what extent, the TOR network increases the diffusion of power in the twenty-first century.

To this end, we presented the two main approaches to power in the field of International Relations. The intention was to point out the conceptual "break" between Strange and the traditional theoretical currents in IR, which resulted in the emergence of the notion of structural power. This emergence was responsible for inaugurating the discipline of IPE—largely responsible for uniting the areas of Politics and Economics in a global

[72] According to Nye (2011), this domain possesses inherent characteristics that allow for the "reduction of power differentials" among the various actors who carry out activities within it.

vision of markets and States. It is from this that Strange makes explicit the phenomenon of the diffusion of power.

Another scholar in the field of International Relations who wrote about "diffusion of power" was Joseph Nye Jr. Unlike Strange, Nye had the opportunity to make specific considerations about what he called the "new domain of power": the region of cyberspace. Perhaps for this reason, he currently remains a reference within the field with regard to studies involving Information Technology and International Relations. The discussion surrounding the recent work of the American scholar in this research occurred for two reasons: first, we intended to point out the differences and similarities between the concept of "diffusion of power" in Nye and Strange; second, to briefly present his theoretical study on the cyber domain.

In summary, Strange's concept of "diffusion of power" rests upon the primary structures, which allow space for non-state actors to hold power. This power was defined by her as "structural power." Nye's concept of "diffusion of power," however, does not discuss (at least explicitly) the primary structures: his work points to the diffusion of power fostered by the emergence of non-state actors in the cyber domain (through the reduction of the costs of entry to this domain) and the technologies proper to cyberspace.[73] These actors, at times, have sufficient power to achieve desired outcomes through the inherent resources of cyberspace. For him, these outcomes can occur within or outside this domain. Nevertheless, despite departing from different epistemologies, both phenomena of power diffusion share similarities: the diffusion of power, whether Nye's or Strange's, occurs in a "vertical" direction—from States to non-state actors.

In this chapter, we also grounded our starting point regarding the operationalization of the phenomenon of the diffusion of power according to Strange (1996). In particular, we highlighted the role of the variables in understanding the dimensions of the diffusion of power. These dimensions are three: authority, control, and outcomes.

[73] According to Nye (2011), this domain possesses inherent characteristics that allow for the "reduction of power differentials" among the various actors who carry out activities within it.

Chapter 3

Dark Web and the TOR Anonymous Network

The Dark Web, through the anonymous network The Onion Router (TOR), is the environment in which this dissertation seeks to analyze the diffusion of power. The TOR network is one of the networks that compose the Dark Web, together with other networks that make an active effort to shield communications, such as the Freenet network and the I2P network. Specifically, the technical knowledge of the TOR network and, in general terms, the policies surrounding the anonymity conferred by this communication channel are essential for the analysis of power diffusion. Thus, this chapter grounds the reasons why we believe the Dark Web is the environment within the cyber domain that most challenges the authority of the State and emanates degrees of power to various actors – whether public or private.

We have divided this second chapter into three main parts: the first part addresses the matters necessary to define and contextualize the Dark Web within the universe of the World Wide Web (WWW), part of cyberspace; the second part seeks, in the context of the Dark Web, to present the TOR anonymous network in its technical and political aspects; the third part establishes the TOR anonymous network as a relevant part of the knowledge structure in the 21st century.

In the first part, we will begin with the history of the global computer network, its origin and technical functioning. With this, we seek to show fundamental points for electronic devices to operate within the mesh of the Internet – such as protocols and packet switching. The TCP/IP protocol, for example, was responsible for establishing connections between distinct computers, creating the system of digital information networks. Packet switching refers to the strategic addressing of data that travels across the network. However, it is quite common for individuals to use different technical terms to designate the same thing within the scope of the global computer network. For example, Finklea (2005) points out that users employ the term "world wide web" as a synonym

for “internet,” although they are not the same. To prevent this from occurring, we felt the need to explain, beyond the history of the Internet, different technical terms such as “network,” “Internet,” “WWW,” “Surface Web,” “Deep Web,” “Dark Web,” and “TOR” – in addition to protocols and packet switching. All of these terms are, in some sense, related to each other.

Next, we will present the WWW, commonly known as the “web.” The WWW is one of the application layers that operates through the Internet. And within this layer, according to current classification, there are six different categories of the Web: Surface Web, Opaque Web, Private Web, Proprietary Web, Truly Invisible Web, and Dark Web. The Surface Web is conventional navigation of the WWW (using browsers such as Google Chrome, Mozilla Firefox, Safari, Opera, etc.) through search portals like “Google,” “Yahoo,” and “Bing!” Unlike the Surface Web, the Deep Web is composed of the other five categories – whose content is not indexed by the search engines of the aforementioned portals, meaning they will not appear in a list as results.

The second part aims to present the specific anonymous network for the purposes of analysis in this research – The Onion Router (TOR). According to Finklea (2015), the TOR network, among the anonymous networks that compose the Dark Web, is the largest in terms of number of users and stored content. We will explain its origin, the “onion routing” technique – responsible for encrypting messages and concealing the identities of users –, “Tor Bridges,” which assist in counter-censorship activities; the hidden services inherent to the network, its popularity, and its political aspect. Our objective was to make explicit the aspects of the anonymous network that make it a unique region of cyberspace.

In the third and final part, we sought to ground the reasons that lead us to believe that the TOR network is an important communication channel, and a relevant component of the knowledge structure in the 21st century.

Initially, the Internet was used by a technical elite composed of computer scientists and enthusiasts in the field. During this period, the moment prior to the creation of the “WWW” by Tim Berners-Lee, the navigation “windows” that exist today did not yet exist; to use the Internet, it was necessary to know a minimum of computer language. To create a more user-friendly interface for the Internet, and to solve problems of access to information, Tim Berners-Lee created the HTTP protocol, responsible for founding the World Wide Web (WWW), a system of connecting pages and servers using hyperlinks. In this environment, search engines emerged, such as Google, which navigate the WWW and store copies of pages and content, as well as addresses, on their own servers. On the search site, these engines are capable of showing lists of results based on terms entered in the search bar. Everything not catalogued by these major search engines remains “hidden” in the vast WWW, as they are not shown by these large information “portals.” This hidden content is called the Deep Web. It is in this region that the Dark Web is

classified, and of which the TOR network is a part. Using specific software, it is possible to access this network. The non-state actors whose activities are studied in the final chapter of this dissertation use TOR to carry out their activities.

In other words, the understanding of the technical functioning of the Internet, in order to contextualize and explain the Dark Web and, specifically, the TOR anonymous network, is fundamental in this research for understanding how, and to what extent, the diffusion of power occurs in this region of cyberspace.

3.1 History and Functioning of the Internet up to the World Wide Web

When discussing the identity of the "father of the Internet," many authors and journalists credit this title to the Englishman Tim Berners-Lee, creator of the World Wide Web – a navigation system composed of pages and hyperlinks born in 1990. However, Berners-Lee's role was to create a navigation system with user-friendly interfaces, through texts and windows where one could "jump" between different pages with content. That is, the Internet already existed when he created the Web – what the latter did was to allow greater reach of the global computer network by encompassing new users who lacked knowledge of computer language. (CASTELLS, 2001). For Naughton (1999), the title of "father of the Internet" is quite contested. But, according to him, Paul Baran has the strongest claims. A former employee of the Rand Corporation, Paul Baran was responsible for developing the basic principles behind the network system at the origin of the Internet: digital signals and data packets.[74] At that time, the launch of the Soviet satellite Sputnik fueled the scientific and technological race between the USA and the USSR. (NAUGHTON, 1999). Faced with this scenario, the American Armed Forces invested in research that could develop technologies capable of protecting military communications against possible nuclear attacks.

In 1964, Paul Baran published his research on a communication system based on a distributive network capable of surviving physical attacks.[75] The survival of communi-

[74]According to Naughton (1999), the Rand Corporation was a "think tank" founded primarily by the US Air Force which, in exchange for investments, received relative freedom to conduct research. Many of these major research projects were generally related to the Air Force's area of interest. When Paul Baran arrived at the Rand Corporation in 1959, at the height of the Cold War, he was tasked with investigating the possibility of preserving the systems responsible for strategic command and control weapons in case of physical attacks. There are other relevant names in the trajectory of Internet creation, besides Paul Baran. Banks (2008) recalls the role of Leonard Kleinrock, whose doctoral research on data distribution in a network resulted in a book published in 1964. Ceruzzi and Aspray (2008), in turn, attribute to Donald Davies, a British physicist, the development and coining of the term "packet switching," essential for the construction of a distributed network.

[75]These first communication systems resistant to physical attacks were imagined by Baran in a way that they could resist without dependence on conventional electrical power: "Since destruction of the national electricity grid was an assumed consequence of a nuclear exchange, the transmitter/receivers

cations depended, broadly speaking, on the way in which the nodes (the term he used to designate communication stations) were connected: (a) centralized, with rare survival prospects; (b) decentralized, with low survival prospects; (c) arranged in a distributive network, with high survival prospects.[76] (BARAN, 1964).

The next step would be to use digital signals to traverse the network, since analog signals lose their quality as they travel through the stations.[77] According to Baran (1964), information would be transmitted between nodes using standardized message blocks. These blocks were of equal sizes and formed by data segments. To travel through the network to the final destination, the data blocks were "disassembled" so that their segments would traverse different routes. At the destination, these segments would be reordered to recreate the original message block, which would be read by the receiver. The nodes are of great importance because they would be responsible for choosing the best route for the next segment of the message block, so that all would arrive at the same chosen destination.[78] The reason for all arriving at the same recipient is due to the message block itself: it contains information indicating the beginning of the message, addressing, sender, precedence, "hand-over number," the actual message content in text format, and the end of the message. (BARAN, 1964).

An interesting metaphor that aids the understanding of this process is to imagine that the message, sent by the sender, is like a jigsaw puzzle. Sending the entire picture through the network (the information) proved to be a challenging task for the purposes of that era (maintaining communication channels intact in case of physical attack on infrastructure). It is easier to break up the picture so that, in the end, only the puzzle pieces (data segments) remain. Thus, they are sent individually through the network toward the designated receiver. The different pieces follow the most varied routes, at different speeds, constantly "reading" the table with information about the best route (lowest cost, highest speed). When they arrive at the destination, they are "scrambled," but behind each piece there are instructions about its position to compose the image. The puzzle pieces are "read" and, in this way, it is possible to recreate the complete picture, just as at its origin. The final receiver can then observe the picture in its original format

were to be powered by small generators fuelled by liquid petroleum from a 200-gallon tank buried in the ground beneath each tower. As each relay-tower would consume only fifty watts of electricity, this local supply of fuel would last for at least three months after failure of the grid." (NAUGHTON, 1999, p.105)

[76] See "Annex 3 – Distributive Networks."

[77] Digital signals do not degrade in the same way as analog signals because they are merely sequences of the digits "zero" and "one" – in addition to there being sufficiently simple techniques to check whether a given sequence was transmitted correctly. (NAUGHTON, 1999).

[78] Naughton (1999, p.103) explains that, in order for the nodes to choose the best trajectory for each segment (lowest cost, highest speed), Baran created an algorithm containing a table. In this table was information about how many "hops" remained for the segment to reach the next node (neighboring node). The table thus indicated the best routes at any given time, as it was regularly fed with information about the state of neighboring nodes – so that, if a node dropped out of this mesh, the table was updated to reflect the change and, thus, message blocks were rerouted to other paths.

in the message read.[79]

In sum, two points are central to Baran's work: that the necessary number of connections for each workstation (node) to ensure the survival of the entire network was three (this characteristic, the number of connections guaranteeing survival, he called "redundancy"); and the segmentation of message blocks into smaller data, capable of being transmitted along the network to the final destination through digital signals and varied routes (this characteristic he termed "packet switching").

Baran's original work on packet switching of messages along a distributed network originated the fundamentals behind network communication that made possible the emergence of the Internet – the network made of networks whose reach in the 1990s became global.

3.1.1 The TCP/IP Protocol

The origin of the Internet as we know it is ARPANET – a network developed among scientists and computer enthusiasts spanning five American universities whose studies were funded by the American military. The name of the network derives from the acronym DARPA (Defense Advanced Research Projects Agency). For digital computers to communicate with each other through the network, they must adopt the same set of rules – or protocols.[80] Otherwise, each machine would only understand itself. The fundamental protocol adopted by the ARPANET network for data transfer was TCP/IP. (CANABARRO, 2014).

Two observations about protocols are pertinent. First, the acts of segmenting data into packets and reassembling data packets (so that they become the original message) need to be managed by a set of rules adopted by both the sending and receiving computers. That is, the computers must obey the same rules of segmentation and packet reconstruction. Second, the computers need to know their position and the position of other computers on the network. Each computer is a node, and the set of nodes forms the "network." Therefore, knowing the position of devices on the network allows computers to know the destination of each packet and whether there is still a route to traverse or not.

From ARPANET, the TCP/IP protocol became popular and, thus, became the most widely used for data transfer on networks. (LAKSHMAN; MADHOW, 1997). Its name

[79]This system is somewhat different in the TOR anonymous network: message blocks and data segments also exist, however, the information behind each "puzzle piece" is hidden beneath layers of cryptography – and each layer can only be "read" by a single node. There is no way to read all layers at once. Another difference concerns addressing. Each node would only know the address of the next node to which to send the piece, but not the final node. These and other characteristics compose the technology of the TOR network that differentiates it from the Internet network – and, thus, attempts to protect messages and users. More on this in later sections.

[80]According to Ceruzzi and Aspray (2008, p.11), "[t]he information that enveloped an electronic packet also had to obey certain conventions, regardless of the contents of the packet. These conventions were called protocols, from the Greek word meaning the leaf glued to a scroll that identified its contents."

comes from the combination of two specific protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP). This protocol ensures the sending, transit, and arrival of packets through a specific set of rules at each moment of data transfer. This set of rules is adopted by all computers on the network. The rules act upon (a) the segmentation of the message block into smaller parcels – these are the data packets that travel through the network; (b) the addressing procedure for each parcel (departure and arrival); (c) the transit of packets through the best routes (lowest cost, highest speed) on the network to the final destination; (d) the orderly and complete assembly of packets at the final destination, so as to obtain the original message block. (CANABARRO, 2014).

Naughton (1999) explains the functioning of TCP/IP in a manner similar to the jigsaw puzzle example, where the overall image is divided into smaller pieces (puzzle pieces) that travel through the network individually and are reassembled only at the final destination to produce the original overall image. He recounts the experience of performing a search on the AltaVista search engine (an information "portal" of the web), quite popular in the 1990s, analyzing the procedures of his computer and the network in sending and receiving data packets. He states:

> The Internet is thus one enormous game of pass-the-packet played by hundreds of thousands of computers, all of them speaking TCP/IP unto one another. It's what engineers call a "packet-switched" system. As each of my AltaVista packets was passed along the system, every computer which handled it scanned the destination address on the 'envelope', concluded that it was addressed to another machine and passed it on in my general direction until it eventually arrived at my computer. This means that each packet may have travelled via a different route. It also means that because some routes are more congested than others, the packets may have arrived in a different order from that in which they were dispatched. But the TCP program on my computer can handle all that: it checks the packets in, uses the information on their envelopes to assemble them in the correct order, requests retransmission of any which have got lost in the post, as it were, and then passes the assembled message to Netscape for display on my screen. (NAUGHTON, 1999, p.21).

But the TCP/IP protocol is not the only protocol used on the network. Two of the earliest protocols were the TELNET Protocol and the File Transfer Protocol (FTP) – asymmetric (unilateral) protocols that allowed the exchange of files from a server computer to a client computer. Subsequently, the Network Control Protocol (NCP) emerged, the first interprocess communication software of ARPANET and a symmetric protocol – that is, it allows the establishment of communication between devices from either the

server or the client computer.[81] The Message Transmission Protocol (MTP) also emerged, which dealt with electronic messages (electronic mails or e-mails). (NAUGHTON, 1999). During this initial period of network development (which would become worldwide), computer scientists and enthusiasts worked in an open and collaborative manner in creating protocols that could be adopted by all machines on the network so that they would use the same "language" to exchange specific information. This characteristic, of open and collaborative work, is highlighted by Castells and Cardoso (2005) as essential for the Internet to become open and plural. In addition to those already mentioned, other protocols still used today include: Hyper Text Transport Protocol (HTTP), Uniform Resource Locator (URL), Simple Mail Transfer Protocol (SMTP), Domain Name System (DNS), Internet Message Access Protocol (IMAP), Internet Relay Chat Protocol (IRC), Media Transfer Protocol (MTP), Voice Over Internet Protocol (VOIP), and others.

When Tim Berners-Lee created the web navigation system in 1990, with addresses, pages, and hyperlinks, using a browser, the Internet was already real. Various digital computers located in different geographical regions were transmitting data and information among themselves. Enthusiasts and academics exchanged files and images, maintained voice connections, sent and received instant messages ("Chats") and emails, among other things. The World Wide Web, therefore, was built upon already consolidated foundations, operating over an existing Internet. Its main characteristic was perhaps making the experience of using the Internet sensorial, enabling the user to "navigate" between windows and content with the click of a mouse.

3.1.2 The World Wide Web (WWW)

The Briton Tim Berners-Lee worked at CERN[82] at the end of the 1980s and developed the web in the months between March 1989 and November 1990. Initially, Berners-Lee identified a problem in the work environment: the research center had great difficulties with the storage and transmission of information and documents among scientists. To "worsen" this situation, the scientists worked in a system of high turnover, since many were there for a limited period of time. This problem hindered, to a great extent, the efficiency of research and of CERN in general. The solution, found by Berners-Lee, was to create an interconnected information system. To build this system, he made use of the young Internet, a network for transmitting data over long distances that uses digital computers. (NAUGHTON, 1999).

[81] The NCP protocol was later replaced by the TCP/IP protocol. (NAUGHTON, 1999).

[82] The acronym CERN derives from the French *Conseil Européen pour la Recherche Nucléaire*, and is an organization better known by its English name, the European Organization for Nuclear Research (CERN). CERN is the European organization for nuclear research, founded in 1954 on the French-Swiss border. Initially, it was concerned with studies related to the atom, but currently it dedicates itself to research related primarily to particle physics. (EUROPEAN COUNCIL FOR NUCLEAR RESEARCH, 2017).

In November 1990, in an attempt to operationalize this solution, Berners-Lee began programming activities and developed a software – which he called a "browser" or "navigator." This software, in practice, created a virtual "window" on the computer's interface that displayed the structure of cyberspace. (Ibid., 1999).

But the browser alone was not sufficient. Naughton (1999) argues that the creator of the Web needed to ensure that public information, stored on other computers on the network, could be accessed through the browser he had created. For this, he began developing a set of protocols that operated on top of the browser he had already created. Thus, if all computers adopted the same languages for the "window" system (browsers) that he had created, these different digital computers inhabiting the global network could communicate with each other through the browser itself. That is, communication between them could happen solely through the "windows."

In particular, two protocols and a dedicated language were essential for the functioning of the Web beyond the browser software: (1) a first protocol to specify the location of information storage within computers (this protocol was analogous to the IP protocol – which specifies the location of each machine connected to the global computer network), which Berners-Lee called the "Uniform Resource Locator" (URL); (2) a second protocol to specify how information should be exchanged between machines (this protocol was also analogous to the FTP protocol – which specifies how files are transmitted on the global computer network), which he called the "Hyper Text Transport Protocol" (HTTP); (3) and a dedicated computer language that he called Hyper Text Mark-up Language (HTML), which became the "idiom" of the entire Web he created. Between the conception of the idea and the creation of the browser (and inherent protocols), the creator of the Web took just over one year. (Ibid., p.239–240).

The Web developed by Berners-Lee became public in January 1991. At that time, it was merely one among the various other applications traversing the network – which, however, had not yet gained popularity.[83] (Ibid.). It is worth remembering that the Internet already existed and was in use at the time of the Briton's creation. Despite the lack of browsers, or user-friendly interface "windows," users who already operated on the Internet were capable of transmitting information and data between computers – all that was needed was technical knowledge and programming language. This fact, Ceruzzi (2008) recalls, is one of the points that kept the Internet, until that moment, as an elitist means of communication – even though it was grounded in a culture of freedom and the sense of community that involved academics and computer enthusiasts, especially

[83]Naughton (1999, p.248) presents a table showing, proportionally, the traffic of protocols used on the backbone of the National Science Foundation (NSF) Internet – that is, the main Internet backbone at the time. In 1993, the FTP protocol was the most used, comprising 42.9% of data traffic. Meanwhile, the Web protocol was responsible for 0.5% of data traffic. Two years later, in 1995, the FTP protocol comprised 24.2% of data traffic, while the Web protocol accounted for approximately 23.9% – becoming the most used protocol on the global computer network. See ANNEX 4 – Data Traffic by Protocol on the "NSF Internet Backbone."

at its origin. It was Marc Andreessen who enhanced the navigation system created by Tim Berners-Lee and brought a world of colors, images, and videos to the interactive "window," enabling the Internet to become popular.

In January 1993, Marc Andreessen made the Mosaic browser public. He was its co-creator, together with Eric Bina. (CERUZZI, 2003). This new software, besides being free, brought other novelties: it was possible to attach images to texts in the navigation window and it could be installed on simple computers – unlike the UNIX workstations, which were very popular. (NAUGHTON, 1999). Andreessen aimed to eliminate the remaining obstacles separating the elite of computer enthusiasts from the general public. And he succeeded because, from Mosaic onward, the Web "application" occupied the greater part of the global computer network. The creators of the Mosaic browser were also responsible for developing the Netscape Navigator, a progressive version of Mosaic: visually "cleaner," secure, with support for elegant layouts and elaborate documents, as well as being much faster. (Ibid., 1999). The Netscape Navigator was commercialized and went public on the stock exchange on August 8, 1995. By the end of that day, each share cost 58 US dollars; a few months later, each share cost 150 US dollars. (CERUZZI, 2003).

The creation of the WWW by Tim Berners-Lee, the Mosaic and Netscape Navigator browsers created by Marc Andreessen, and the widespread adoption of the TCP/IP and DNS protocols are the technical developments that allowed the Internet to expand and take on worldwide contours, since its use became simple for the portion of individuals who do not deal with computing directly. (CANABARRO, 2014). Another aspect, albeit non-technical, that contributed to this was the commercialization of the Internet: "From the commercialization of network access service as a political-economic development of the Digital Age, the use of the Internet came to encompass the most varied areas of human life activity and, with this, to have socioeconomic, political and cultural implications [...]." (CANABARRO, 2014, p.94).

Naturally, with a visually friendly Internet, available for navigation by the general public (and no longer only by enthusiasts), open to commercialization, accessible through browsers that brought texts, figures, and dynamism to the network, the next step was the development of major search engines such as AltaVista, Yahoo!, and Google. These "engines" were responsible for performing searches across the vast quantity of information available on the Web. That is, they were navigation "facilitators": instead of the user individually searching each page for content of interest, these engines provided a list of pages as the result of a search by terms defined by the user. Everything that was listed as a result later became known as the Surface Web. Everything that remained beyond, and therefore did not appear in any results listing of any search engine, became known in the literature on the subject as the Deep Web. These will be the topics addressed in the next subsection.

3.2 Surface Web and Deep Web: The Parting of Digital Waters

In September 2001, Michael K. Bergman, a researcher at Bright Planet, published an article entitled *The Deep Web: Surfacing Hidden Value* dealing specifically with the Deep Web.[84] In the article, Bergman (2001) states that he conducted the research based on data collection carried out between March 13 and 30, 2000, and acknowledges that his research is the first study to quantify and characterize the Deep Web. According to him, the Deep Web refers to the informational content available on the Web that is not indexed, or searchable, by conventional search engines.[85]

We highlight four points from the research conducted by Bergman (2001): (1) the study sought to quantify the size of the Deep Web and concluded that it is approximately 400 to 550 times larger than the Surface Web; (2) general characteristics of the Deep Web involve the size of its pages, much larger than Surface Web pages, and the size of its documents, approximately 27% smaller than Surface Web documents – in addition to indicating that approximately 97.4% of the Deep Web consists of public pages accessible without restriction; (3) search engines adopt criteria for the indexing of pages in their databases – and, consequently, criteria for not indexing many Web pages; (4) the data is old, from the year 2000, but due to the scarcity of quantitative studies on this subject, they remain relevant as a starting point.[86]

In Brazil, Fidêncio and Monteiro (2013) identify the literature of Bergman (2001) and Sherman and Price (2001) as the foundations upon which further studies on the subject were developed. According to them, Bergman (2001) was responsible for providing the quantitative dimension of the Deep Web, while Sherman and Price (2001) sought to categorize it. The latter gave rise to four classifications of "invisibility"[87]: Opaque Web;

[84]This article became a reference in studies on the subject of the Deep Web, listed as the most cited article by the "SCOPUS" database in 2017, using the term (in quotation marks) "Deep Web."

[85]The researcher opts for the use of the term "Deep Web" instead of the term "Invisible Web," coined by Jills Ellsworth in 1994, to designate the informational content "invisible" to conventional search engines. According to Bergman (2001), this content is "visible" and accessible through non-conventional methods. For this reason, he abandons the term and adopts "Deep Web." However, Sherman and Price (2001) use the original term "Invisible Web" to refer to the same object (also using the term "dark matter," which should not be confused with the term "Dark Web" or "Darknet"), in addition to categorizing the "Invisible Web" into four regions.

[86]Bergman (2001, p.1) indicates that the Deep Web contains approximately 7,500 terabytes of information compared to 19 terabytes of information on the Surface Web. In terms of individual documents, the Deep Web contains approximately 550 billion documents – while the Surface Web comprises approximately 1 billion individual documents. The studies of Sherman and Price (2001, p.82) indicate other data: excluding special search tools and data irrelevant to researchers (or users who perform searches), it is estimated that the "Invisible Web" is between 2 to 50 times larger than the "Visible Web." However, other quantitative research on the subject was also conducted by He et al (2007).

[87]It is worth remembering that Sherman and Price (2001) use the term "Invisible Web" to refer to what Bergman (2001) calls "Deep Web" – the reason they named the four categories they defined according to degrees of "visibility." The term "Deep Web" became popularized.

Private Web; Proprietary Web; and Invisible Web.[88] According to the authors, "We make these distinctions not so much to make hard and fast distinctions between the types, but rather to help illustrate the amorphous boundary of the Invisible Web that makes defining it in concrete terms so difficult." (SHERMAN; PRICE, 2001, p.293). The "Dark Web" category was described by Becket (2009).

Below follows a description of the four distinct Webs described by Sherman and Price (2001) and, subsequently, a description of the "Dark Web" as defined by Becket (2009).

3.2.1 Opaque Web

According to Sherman and Price (2001), the Opaque Web is composed of files that have not been included in the indexes of search engines despite being technically capable of inclusion. That is, there is no technical obstacle preventing this content from being indexed.

There are reasons why this informational content is not indexed by search engines, and the researchers list four: (1) the depth of reach of the "robots,"[89] since there is a cost involved in the "sweep" of the Web by the search engine; (2) frequency of the sweep – the web has a dynamic character, with countless pages being added daily, which means that each search engine must make decisions about the frequency of sweeps performed by the "robots" that carry out page indexing. The "robots" must verify that the page is still valid, or update it in their index; (3) maximum number of visible results – each search engine determines the maximum quantity of results listed for the user in each search; (4) disconnected URLs – pages that are not submitted directly to search engines and that do not have external links on other pages pointing to them are called "disconnected URLs" and cannot be indexed because the robot has no way of finding them.

In summary, Sherman and Price (2001) conclude by stating that "[...] the Opaque Web is large, but is not impenetrable. Determined searchers can often find material on the Opaque Web, and search engines are constantly improving their methods for locating and indexing Opaque Web material." (Ibid., p.296).

3.2.2 Private Web

The Private Web consists of Web pages that are technically possible to index by search engines but that were deliberately excluded from them. The Private Web, in general, is

[88] Fidêncio and Monteiro (2013) created a schematic figure based on the literature of Sherman and Price (2001), adapted from a scheme similar to that of Ford and Mansuriam (2006). See "ANNEX 5 – The Various Webs."

[89] According to the authors, search engines launch "robots" (software programs) that perform a "sweep" of the Web, accessing pages upon pages (jumping between them through hyperlinks) and copying and listing these pages in large databases. These robots are also known as "spiders" (since their function is to crawl through the "web"). Another name used is "crawlers." (SHERMAN; PRICE, 2001, p.15).

composed of regions of the Web whose access is not public – only users with permissions may access the pages. (Ibid., p.73). Furthermore, there are three ways to exclude a page from the reach of search engines: (1) implement the use of a password to access the page's content, since the robots that perform web sweeps cannot overcome this obstacle; (2) use the text file "robots.txt"[90] to inform the sweeping robot not to index the page; (3) use the "no index" meta tag[91] to prevent the sweeping robot from reading beyond the page's header content and, thus, indexing the body of the page.

The researchers further emphasize that the first method, the implementation of a password for access, is a stronger technique compared to the other two because it makes use of a specifically technical barrier, as opposed to a voluntary standard.

3.2.3 Proprietary Web

The "Proprietary Web" is composed of pages whose access is only permitted through agreements to special terms. That is, search engines cannot index them because their access depends on these terms (accepted in exchange for viewing the content). This category includes content accessible through free registrations; paid registrations through a fee; subscription registration for content access; "newsletter" subscriptions; etc. The sweeping "robots" cannot satisfy even the simplest registration requirements and, for this reason, are unable to index the content of pages behind the registration/subscription screen. (SHERMAN; PRICE, 2001, p.296). The authors also offer some examples of pages that belong to the "Proprietary Web" category.

3.2.4 Truly Invisible Web

The authors call the "Invisible Web" also the "Truly Invisible Web." This is done so as not to confuse the reader between the terms "Invisible Web" (within which are the categories "Opaque Web," "Private Web," "Proprietary Web," and "Truly Invisible Web").

They emphasize the care needed with the definition of the "Truly Invisible Web" category, as such a definition must be fluid so as to cover new formats of documents

[90] Sherman and Price (2001) discuss robots and seek to define them as follows: "The Robots Exclusion Protocol is a set of rules that enables a Webmaster to specify which parts of a server are open to search engine crawlers, and which parts are off-limits. The Webmaster simply creates a list of files or directories that should not be crawled or indexed, and saves this list on the server in a file named robots.txt. This optional file, stored by convention at the top level of a Web site, is nothing more than a polite request to the crawler to keep out, but most major search engines respect the protocol and will not index files specified in robots.txt." (SHERMAN; PRICE, 2001, p.63)

[91] Specifically on this point, they argue that "The second means of preventing a page from being indexed works in the same way as the robots.txt file, but is page-specific. Webmasters can prevent a page from being crawled by including a 'noindex' meta tag instruction in the 'head' portion of the document. Either robots.txt or the noindex meta tag can be used to block crawlers. The only difference between the two is that the noindex meta tag is page specific, while the robots.txt file can be used to prevent indexing of individual pages, groups of files, or even entire Web sites." (SHERMAN; PRICE, 2001, p.63)

and pages – since the sweeping robots of search engines are in constant adaptation and technological progression. In this sense, the researchers highlight three main sources of informational content belonging to the "Truly Invisible Web" category: (1) Web pages whose format is not yet managed by the current category of sweeping robots, which according to them involve documents in "PDF," "Shockwave," "PostScript," "Flash" formats, etc.[92]; (2) dynamically generated Web pages, specifically from a request that uses a non-interactive "script" to generate the page[93]; (3) informational content stored in relational databases[94], as there is no way to extract the information without making an inquiry to the database.

3.2.5 Dark Web

The "Dark Web," often understood as "Darknet," is not part of the initial categories defined by Sherman and Price (2001). Fidêncio and Monteiro (2013) note that this new "part" of the Web appears later in the literature with Andy Becket, in an article published by the newspaper "The Guardian," in the Technology section, in 2009.[95]

Specifically, the Dark Web comprises content that has been intentionally hidden from third parties. (FINKLEA, 2015). Another similar definition, raised by Becket (2009), is that the Darknet is an online network hidden from non-users. Biddle et al (2002) state that the Darknet is "a collection of networks and technologies used to share digital content [...] not a separate physical network but an application and protocol layer riding on existing networks." (BIDDLE et al, 2002, p.1). For the purposes of defining

[92]At the time the book was written, in 2001.

[93]The problem, according to the authors, is the indiscriminate use of "scripts" that lead sweeping robots into "spider traps" in which they become literally stuck within a set of thousands, or millions, of pages solely to drive away search engines. (SHERMAN; PRICE, 2001, p.74–75). According to the definition by Tech Terms (2017), "A computer script is a list of commands that are executed by a certain program or scripting engine. Scripts may be used to automate processes on a local computer or to generate Web pages on the Web." (TECH TERMS, 2017).

[94]"A relational database is a database model that stores data in tables." (TECH TERMS, 2017).

[95]Two observations regarding the term "Dark Web." This term was also used by Hsinchun Chen, a professor at the University of Arizona, director and founder of the Artificial Intelligence Laboratory (AI LAB), in 2006, in the work *Intelligence and Security Informatics for International Security*. The meaning given by Professor Chen is different. He uses the term "Dark Web" to designate research, in the field of computer science, related to the phenomenon of terrorism – especially within the scope of the "Dark Web Portal" project. Another meaning of the term "Dark Web" was given by the co-founder of TOR software, Roger Dingledine, during the "DEF CON Hacking" convention in July 2017. On that occasion, Dingledine was criticizing journalists who presented the TOR software as a space dominated by illicit services (which, according to him, only represents the activities of 3% of the TOR network's users). To these illicit services, on that occasion, Dingledine called "Dark Web" – stating that this "Dark Web" did not exist [proportionally]. (THOMSON, 2017). Researcher Mary McEvoy Manjikian also used the term in this sense, stating "In the days and weeks after September 11, the description of the Internet as a dichotomous world consisting of both a 'dark web', which unregulated, shadowy, and prone to harbor criminal behavior, and more open public web, gained prominence." (MANJIKIAN, 2010). Finally, the term "Darknet" is used by the Freenet project to indicate the anonymous network installed between friend nodes, as opposed to "Opennet" which is an anonymous network installed between stranger nodes. (FREENET, 2017). In this research, we will use the term in the sense given by Finklea (2015).

this research, Dark Web designates the set of anonymous online networks that make an active effort to remain hidden from non-users, using, for this purpose, an application and protocol layer created over existing physical networks. For this reason, the Dark Web is composed of anonymous networks – such as the Freenet, The Onion Router (TOR), and The Invisible Internet Project (I2P) networks.[96]

Despite not being part of the categories initially described by Sherman and Price (2001), Fidêncio and Monteiro (2013) make an attempt to contextualize it within their writings: "[...] it is quite safe to consider the Dark Web as a new branch of the Invisible Web [as defined by Sherman and Price (2001)]: its characteristics are its own; its philosophy is its own and, above all, its content is the most enigmatic and disordered of all the branches." (FIDÊNCIO; MONTEIRO, 2013, p.692). And they complement, further stating that "In the Dark Web, anonymity is desirable to users, mainly because of philosophical positions of users or some position contrary to social norms." (Ibid., p.693).

The definition of "Dark Web" used in this research finds its origin in an article by Andy Becket, 2009, which states that "the dark web is part of the Internet that cannot be accessed by mainstream software. It includes hidden sites that end in '.onion' or '.i2p' or other Top-Level Domain Names only available through modified browsers or special software."[97] (GEHL, 2016, p.1220). Along these lines, Chertoff and Simon (2015), from Chatham House, The Royal Institute of International Affairs, adopt the meaning of "the portion of the deep web that has been intentionally hidden and is inaccessible through standard Web browsers [...] Dark Web sites serve as a platform for Internet users for whom anonymity is essential, since they not only provide protection from unauthorized users, but also usually include encryption to prevent monitoring." (CHERTOFF; SIMON, 2015, p.3). These ideas are complemented by later works such as that of Devine, Egger-Sider, and Rojas (2015). They also affirm that the Dark Web is a smaller portion of the Deep Web that was intentionally hidden and, for this reason, becomes inaccessible through conventional web browsers.

Finklea (2015) also uses the concept in the sense that the Dark Web is one of the regions of the Deep Web that contains content that was intentionally hidden and whose users can access through the use of special software like TOR. Furthermore, she states that this region can be accessed for legitimate purposes and to hide malicious or criminal activities, and that it was the exploitation of the Dark Web for illegal practices that gained the interest of authorities and policymakers. Roche (2016) identifies the Dark

[96]The origin of the Dark Web refers to the creation of the first anonymous network – in this case, the Freenet network. Based on the final course work in Computer Science and Artificial Intelligence by Ian Clarke: "A Distributed Decentralised Information Storage and Retrieval System," from 1999, at the University of Edinburgh. The Freenet network, accessed through software of the same name, was launched the following year.

[97]The suffix ".onion" indicates navigation of content from the TOR online network, accessed by non-conventional software of the same name. The suffix ".i2p" indicates navigation of content from the I2P online network, also accessed by non-conventional software of the same name.

Web as a hidden world behind encryption, peer-to-peer technologies, and anonymity that mask IP addresses to conceal the user's location.

To access the Dark Web, the use of certain "tools" is necessary – used by human rights activists to create an online communication system on wireless mesh networks – such as the free software TOR, which provides anonymity, the peer-to-peer platform I2P, the Freenet software, and the Darknet Project. Researchers Zulkarnine et al (2016, p.109) highlight the characteristics of the Dark Web.[98] These are: decentralization, the use of Internet infrastructure, and the use of non-conventional protocols and ports that are unreachable by those outside the network. In law, the study of Ghappour (2017, p.1077) stands out, defining the Dark Web as a global network of computers that use encrypted protocols to communicate, allowing users to conduct transactions anonymously without revealing their locations.

Thus, we raise four important points common to the definitions identified in this section: (1) the Dark Web is part of the Deep Web; (2) it corresponds to a region of the Web that is intentionally hidden; (3) to access it, the use of non-conventional navigation software is necessary; (4) it uses anonymity to shield communications and the user's location from third parties.

In this manner, from the definitions examined, we use the following concept of "Dark Web": a region of the Deep Web composed of online networks, hidden from non-users and that use anonymity to shield communication and user location, whose access is through non-conventional navigation software. (BECKET, 2009; CHERTOFF, SIMON, 2015; DEVINE, EGGER-SIDER, ROJAS, 2015; FINKLEA, 2015; GEHL, 2016; ROCHE, 2016; GHAPPOUR, 2017). We note, however, the existence of other definitions, not adopted by this research, but which are also discussed in the literature on the topic.[99]

Three networks form part of the Dark Web, as defined above: the pioneering "Freenet," which emerged in 2000; the "TOR" network, which was born in 2002; and the "I2P" net-

[98] According to them, the Dark Web is built on top of the public Internet.

[99] Biddle et al (2002) define the "Darknet" as a network that emerges from the broad exchange of objects that can be copied and distributed among network users connected by high-bandwidth channels. The idea is to capture the notion of mass distribution of objects among thousands or millions of users. Everett (2009) elucidates distinctions between the terms "Dark Internet," "Dark Web," and "Darknets." According to her, "The term 'dark internet' is used to describe any network host that appears to be unreachable using conventional online means – even though it sits on the conventional internet. [...] Separate from this is the 'dark web', otherwise known as the 'deep web'. In the same way that the web is a subset of the internet, the dark web is also a subset of the dark internet. Therefore, the phrase denotes any web server that cannot be found using regular search engines such as Google. [...] The final category comprises darknets. These are networks that comprise multiple dark servers and are used by everyone from political activists to cybercriminals and international intelligence service agencies in order to covertly communicate, swap information and undertake commerce online. These dark hosts are connected by mesh-based Usenets or peer-to-peer filesharing networks using non-standard communications protocols (rather than HTTP) to enable users to deliver encrypted and generally anonymised information in a way that is difficult to detect and trace." (EVERETT, 2009, p.10). Pace (2016) synthesizes the definitions of Everett (2009) and concludes that the "Dark Web is an amorphous collection of Internet sites that run on darknets, or overlay networks that employ non-standard communication protocols in order to encrypt and anonymize information." (PACE, 2016, p.2–3).

work, whose origin was in 2003. For research delimitation purposes, we opted to analyze, specifically, the TOR network. For Moore and Rid (2016, p.9), the "Tor Project," responsible for managing the network, is one of the most controversial and sophisticated encryption platforms of our time. According to the authors, "the fluid architecture of these networks [Freenet, I2P, and TOR] makes size estimation difficult, but it seems that TOR is the largest [network], with I2P in a distant second place. Others are significantly smaller in scope and popularity." (MOORE; RID, 2016, p.15, our translation).

In the next section, we will address in detail the TOR network covering the following topics: what the network is; what it serves; its development history; technical functioning; "hidden services" (or, according to the literature on the subject, "hidden services"); popularity; political aspect and specific characteristics. The objective is to describe its political importance (which interests us) based on its history, functioning, and current popularity.

3.3 The Dark Web Through the TOR Network

The Onion Router (TOR) network is a low-latency "anonymization" network for TCP traffic.[100] (DINGLEDINE, MATTHEWSON, 2005; PACHENKO, PIMENIDIS, RENNER, 2008; EDMAN, SYVERSON, 2009; CHAABANE, MANILS, KAAFAR, 2010; HOPPER, VASSERMAN, CHAN-TIN, 2010; LI et al, 2010; LI et al, 2011; ALSABAH, BAUER, GOLDBERG, 2012; MOGHADDAM et al, 2012). In other words, it is an anonymous communication network with thousands of router nodes around the world.[101] (EDMAN; SYVERSON, 2009). The anonymous character of this digital communication system allows its users to navigate the Internet without revealing their identities or locations. (LOESING, MURDOCH, DINGLEDINE, 2010; ELAHI et al, 2012). In practice, it constitutes a popular privacy enhancement system that is designed to protect the privacy of its users against traffic analysis attacks launched by a non-global adversary.[102] (MCCOY et al, 2008, p.63). Furthermore, TOR was designed to operate on TCP applications – such as the Web and instant messaging, for example. (LI et al, 2010). For this rea-

[100] Which confers anonymity.

[101] The TOR network uses the infrastructure of the global computer network itself, operating on data traffic – the responsibility of the TCP protocol – and is based "on a client-server architecture model." (ALSABAH; BAUER; GOLDBERG, 2012, p.74). In practice, this means that the network uses the same basic principles of the protocol for data traffic as the Internet itself (for this reason, we say it uses the same infrastructure).

[102] Using the Internet means that the data from your machine travels the global computer network efficiently. This is what enables navigation. In the search for the identity of network users, agents launch attacks on data traffic. In this way, the traffic is analyzed (behavior, intensity, route, etc.) in an attempt to establish a pattern and, thus, facilitate the identification of users. Edman and Syverson (2009, p.380) explain this in more detail by stating that "Tor aims to provide anonymity to clients by sending multiply-encrypted data packets through a series of relays distributed across the Internet. Each relay removes a layer of encryption and forwards the result on to either another relay or to the client's intended destination, such as a website."

son, its use is intended for Web "navigation" and, therefore, we say it is a "low-latency" network.

The origin of TOR derives from a collaborative project between the non-profit organization "Free Haven Project"[103] and the United States Naval Research Laboratory, under the United States Office of Naval Research, funded by the Defense Advanced Research Projects Agency (DARPA). (DINGLEDINE; MATHEWSON; SYVERSON, 2007). The objective of this collaborative project was to create a distributive, anonymous, encrypted network that would be easy to implement so that it could be used by those who needed it. The TOR network was offered as a free service to promote unrestricted access to the Internet in locations where strong online censorship occurred, or where the threat of persecution of those seeking access to locally illegal information was real. (MOORE; RID, 2016). The TOR software was developed in September 2002. (AKHOONDI; YU; MADHYASTHA, 2012). Its launch was in 2003. (ELAHI et al, 2012; DINGLEDINE; MATTHEWSON; SYVERSON, 2007). In 2005, two years after its launch, the Electronic Frontier Foundation (EFF) decided to fund the efforts of the Free Haven Project for one year, with the objective of helping to maintain the civil liberties of ordinary citizens in the cyber domain. Since 2006, the Tor Project has become a non-profit organization and has been funded by groups committed to activism around online blocking and Internet censorship.[104] (DINGLEDINE; MATTHEWSON; SYVERSON, 2007).

In sum, the software was conceived through a collaborative project between civil society, in the figure of the Free Haven Project organization, and the State – through the United States Naval Research Laboratory, whose funding was provided by DARPA. It is worth remembering that DARPA also participated in the creation and progress of the Internet in previous decades.

Next, we will discuss the history of the development of the TOR software followed by its functioning; the "hidden services" that generate "unexpected" consequences of the tool's use; the popularity of the TOR software and its political character in the 21st century; general characteristics; and, finally, the knowledge structure in the 21st century and the cyberpower that originates from cyberspace. The objective is to describe the ideological and creative processes that enabled the implementation of this anonymous communication system at the global level, affecting the political actions of public and private groups. Furthermore, for informational purposes, we seek to describe the nature of the developed technology that enables its functioning and effectiveness. This holistic view of the network's progress allows us to make some considerations about the knowledge structure and the "power" that operates in cyberspace.

[103]The "Free Haven Project" began in 1999 as a research project composed of students from the Massachusetts Institute of Technology (MIT) with the original objective of creating a free and functional data haven. (FREE HAVEN, 2017).

[104]Such as the groups "Omidyar Network" and "The US International Broadcasting Bureau." (DINGLEDINE; MATTHEWSON; SYVERSON, 2007).

3.3.1 History and Development of TOR

> The Free Haven Project intends to deploy a system that provides a good infrastructure for anonymous publication. Specifically, this means that the publisher of a given document should not be known; that clients requesting the document should not have to identify themselves to anyone; and that the current location of the document should not be known. (FREE HAVEN, 2017).

Initially, "The Free Haven Project" researched ways to implement a system capable of offering anonymous publication. Subsequently, the objectives expanded to include an anonymous communication system – and not merely publication. Curiously, the individuals responsible for the implementation – Roger Dingledine,[105] Nick Mathewson,[106] and Paul Syverson[107] – realized that not only was publishing anonymously interesting and necessary, but also maintaining Internet communications anonymously.[108] The result was the implementation and public launch of the TOR software in 2003, based on the "onion routing" design that had already been discussed at the end of the 1990s.[109] The software implemented "onion routing" technology that sits upon the routing of data flows, handled by the TCP protocol, through "chosen paths in a network of routers using layered encryption and decryption of the content."[110] (PACHENKO; PIMENIDIS; RENNER, 2008, p.221). It should be noted, however, that the software has undergone various modifications since its original launch with the objective of implementing improvements in terms of security, efficiency, and deployment. (EDMAN; SYVERSON, 2009, p.381).

We perceive, therefore, that the "onion routing" design is concerned, essentially, with the privacy and anonymity of information and users. This first notion about anonymous

[105] Member of "The TOR Project." (DINGLEDINE; MATHEWSON; SYVERSON, 2007).

[106] Member of "The TOR Project." (DINGLEDINE; MATHEWSON; SYVERSON, 2007).

[107] Member of the "US Naval Research Laboratory." (DINGLEDINE; MATHEWSON; SYVERSON, 2007).

[108] Subsequently, the TOR software was implemented with the possibility of anonymous Internet communication and also anonymous Web navigation.

[109] The reason why Dingledine, Mathewson, and Syverson categorize TOR as part of the third generation of implemented "onion routing" designs. (DINGLEDINE; MATHEWSON; SYVERSON, 2007).

[110] In simplified terms: the idea is that data flows are encapsulated in layers of cryptography. These layers resemble an "onion," the origin of its name. These data, encapsulated in layers of cryptography, travel (according to the TCP protocol – specific to the control of data transmission) through the infrastructure of the global network using a "path" that can be chosen. This path is chosen because, within it, there exist specific routers (called "onion routers") that are specific to this network (which is a type of "onion routing network"). The choice occurs among which of these onion routers to use. By definition, these onion routers use layers of encryption and decryption – that is, they can remove the cryptographic layers from each data packet (the "capsules" that surround the data packet). (ELAHI et al, 2012, p.43–44). Specifically regarding TOR routers, "A Tor router can modify the decrypted contents of a message entering or leaving the network. Indeed, in the past, routers have been caught modifying traffic (i.e., injecting advertisements or performing man-in-the-middle attacks) in transit, and techniques have been developed to detect this behavior." (MCCOY et al, 2008, p.69). More details in the functioning section.

communication schemes was originally introduced by Chaum in 1981.[111] (HOPPER; VASSERMAN; CHAN-TIN, 2010). In this sense, anonymity is defined as:

> Anonymity is defined as a state in which an agent is not identifiable within an anonymity set. The anonymity set is a system of senders, receivers, and servers in the communication network. [...] Anonymity is a combination of both unidentifiability, i.e., observers can not identify any individual agent, and unlinkability, i.e., observers can not link an agent to a specific message or action. (LI et al, 2011, p.1).

In the cyber domain, the concern is with identifying the user or the possibility of tracking their activities and, thus, connecting the subject to the action. Anonymity has always been a dichotomous subject in social life and in cyberspace. (LI et al, 2010, p.2). It can be used for two purposes. First, it can be used by an agent who, depending on their activities, confers a "peaceful," protective, and legitimate "aura," or equally, it can be used to enhance illicit and criminal attitudes and behaviors.[112] The advent of new communication technologies provides a market for the study and implementation of techniques that shield users and information from espionage – given that, currently, there exist techniques and actions by governments and private companies that aim to "mine" the information traveling through the mass of Internet users. In other words, communication on the global computer network is becoming increasingly less private. (MITTAL et al, 2011, p.215). The potential privacy invasions are especially threatening to political dissidents, unofficial leaks, and political activists – reasons why anonymous communication systems are in vogue. (Ibid., p.215). The TOR software, in this sense, illuminates the political character of these types of systems because it confers not only anonymity but also strong resistance to censorship. (MOGHADDAM et al, 2012, p.97).

From the need for privacy, two niches emerge in the digital environment of cyberspace: "anonymization" systems and the creation of "anonymizer" services. The latter, according to Li et al (2011, p.1), is a direct product of anonymization systems (of which anonymity networks are a part). Anonymization systems are "community contributed systems" – such as "Java Anon Proxy," "TOR," and "I2P." What they have in common is that they send data packets through "relays" so that no single system has information about both the sender and the receiver. (Ibid., p.2). That is, they form their own networks.

[111] "[Chaum] proposed sending messages through a 'Mix server' that mixes together messages from several senders before forwarding these messages to their destinations, concealing the relationships between senders and receivers." (HOPPER; VASSERMAN; CHAN-TIN, 2010, p.2)

[112] "On one side, anonymous technologies provide legitimate usages such as privacy and freedom of speech, anti-censorship, anonymous tips for law enforcement, and surveys such as evaluation and feedback. On the other view, anonymity technologies provide protection to criminals in facilitating on-line crimes such as piracy, information and identity theft, spam, cyberstalking and even organizing terrorism. Additionally, they may be utilized for Internet abuse for bypassing the Internet use policy of an organization, exposing organization to malicious activities, abusing organization resources, and prevent web filters from monitoring." (LI et al, 2011, p.2)

"Anonymizer" services, on the other hand, allow anonymous navigation by users within the Web, using a conventional browser.[113] It is worth remembering that, in this latter case, because the companies that offer these services on the conventional Web possess all communications, they provide a degree of anonymity considered low to their clients.[114] (Ibid., p.5).

TOR has developed over time and has a history of improvements and implementation of technical novelties, in addition to considerable growth. Since its publication and launch, the TOR network community grew, reaching the mark of 1,500 active routers at any given moment in 2009. (EDMAN; SYVERSON, 2009, p.385). On the Tor Project website, it is possible to verify data on the numbers of users who offer their machines as "routers" for the network (in order to apply "onion routing") from the year 2011 onward: in that year, the number was less than 1 million, reaching nearly 6 million users in the second half of 2013, dropping to fewer than 2 million at the end of 2016 and the beginning of 2017, and finally surpassing the mark of 4 million by the end of 2017.[115] Since mid-2013, the number of users has exceeded 1 million.

In terms of objectives, we see significant changes: at its inception, its goals revolved around two main ideas – preventing attacks from revealing two agents communicating with each other; and preventing such attacks from also revealing the various communications "from" or "to" a single user. (CHAABANE; MANILS; KAAFAR, 2010, p.167). Subsequently, the software gained popularity – especially among users intending to circumvent national censorship systems such as those in Iran and China. (LOESING; MURDOCH; DINGLEDINE, 2010, p.204). Logically, repression against these users was implemented. Thus, one of the main innovations aimed primarily at reaching users in risky situations concerns the implementation of "bridges" for accessing the TOR network. (CHAABANE; MANILS; KAAFAR, 2010). The efforts committed to repairing the network and implementing improvements are continuous and progressive. The very architecture of the network has been altered over time in order to meet these objectives. (MOORE; RID, 2016, p.17).

In the next section, we will describe the functioning of TOR that enables the privacy of communications and anonymity among its users.

[113]These services allow the user to maintain some degree of privacy while navigating the Web by avoiding the collection of information that could identify the user, such as the machine's IP address. Such services are provided by commercial companies, driven by user subscription fees, or non-commercial organizations that profit from advertisements or from services crafted in a homemade fashion through anonymous open-source tools. (LI et al, 2011, p.1). Some of these services were offered commercially, such as "Anonymizer.com" and "Gotrusted.com." (Ibid., p.5). For more information, see LI et al, 2011, p.5.

[114]In summary, the degree of anonymity varies because it depends on the mechanism used by the user, the capabilities of the adversary who wishes to spy on the communication, and the environment of the operation. (LI et al, 2011, p.1).

[115]See APPENDIX 6 – "DIRECTLY CONNECTING USERS."

3.3.2 TOR Software Functioning

In order to understand the basics of TOR functioning, we list seven points that will be discussed in this section: (1) general functioning, which comprises the size of the network in terms of "onion routers" and user behavior; (2) the differences between high and low latency networks; (3) the volume of "BitTorrent" data and what this has to do with the TOR network; (4) why the TOR network is an "application" network; (5) the system based on 3 onion routers; (6) the role of cryptography; (7) general characteristics. We believe that, if we adequately cover the mentioned points, it will be possible to understand the reasons why the TOR software gained popularity among users and became an important political tool in the cyber domain of the 21st century.

In general terms, perhaps the first thing we need to know about anonymous networks is that they function by "hiding" users among users. This means that the larger the network in terms of users, the easier it will be to "mix" these users among each other so that it is more difficult to distinguish them from one another. In other words, when new users join this network, the existing users become more secure – all because the total volume of users has grown. (DINGLEDINE; MATHEWSON, 2005). Furthermore, Dingledine and Mathewson (2005) argue that there is one more "detail" for anonymity to be possible: the users of this network must have similar behaviors, as much as possible, to make it difficult to distinguish between them. (Ibid., p.4). This is the reason the network needs to be accessible to a reasonable number of users (who serve as "onion routers" for this network) with a sufficient degree of usability so that they can use the tool without difficulty and with a similar purpose (to extract similar behaviors from them).[116]

According to Hopper, Vasserman, and Chan-Tin (2010), anonymous networks fall into two categories: high-latency anonymous networks and low-latency anonymous networks.[117] High-latency networks are, for the most part, used by non-interactive applications with the objective of providing a strong degree of "anonymity"; and low-latency networks are used, to a large extent, for anonymous navigation with good performance on the Web. (LI et al, 2010). That is, although high-latency anonymous networks have a "strong" degree of shielding, they are not used for navigation and other applications – which are common, for example, to Web navigation on the Surface Web. The objective of the TOR network is to allow users to navigate and perform other actions derived from applications geared toward Web "navigability." For this reason, there would be incoherence in the design of the TOR network if it were designed as a high-latency network. Given this, the TOR anonymous network is classified as a low-latency anonymous network – that is, beyond anonymity, the navigability of the Web by its users is also prioritized.

[116] If the objective is to provide data confidentiality and storage, one should seek a network that gives priority to this. Similarly, if the objective is privacy of communications, one prioritizes the search for a network whose objective is to provide this.

[117] "High-latency anonymity network" and "low-latency anonymity network." (HOPPER; VASSERMAN; CHAN-TIN, 2010).

(DINGLEDINE et al, 2004; MCCOY et al, 2008; EDMAN, SYVERSON, 2009; LI et al, 2010; HOPPER, VASSERMAN, CHAN-TIN, 2010; MITTAL et al, 2011).

In chronological order, first the high-latency networks were developed, followed by the emergence of low-latency networks. The former provide a high degree of anonymity but, in return, are practical only for non-interactive applications that tolerate delays of many hours. (EDMAN; SYVERSON, 2009). Some of these high-latency systems are Mixmaster and Mixminion, which deliver messages after a delay of approximately 4 hours on average, with the objective of guaranteeing anonymity against a strong adversary capable of observing data traffic and controlling some routers that form part of the anonymity scheme. For this reason, high-latency networks adopt methods that result in delayed data delivery and greater bandwidth consumption – all to "cover up" traffic and make analysis by third parties difficult. (HOPPER; VASSERMAN; CHAN-TIN, 2010). This would be unfeasible for the TOR anonymous network, given that it aims to fulfill purposes of navigability and user communication, while still offering a satisfactory degree of anonymity. Be that as it may, high-latency anonymous networks suffer "side effects," produced by this strong shielding to provide anonymity, that result in delays and bandwidth consumption. For this reason, high-latency networks attract few users. (EDMAN; SYVERSON, 2009).

Subsequently, the low-latency networks emerged. They arose to meet the need for better performance with the sending of data packets in circuits with little processing delay. (MITTAL et al, 2011). The networks that applied the "onion routing" technique, discussed in the literature since at least the beginning of the 1990s, became the most widely used low-latency networks – such as the TOR network and the I2P network.[118] With regard to low-latency networks, this "design" became the most adopted. (LI et al, 2010). Furthermore, as seen previously, they are capable of providing faster performance and, for this reason, are intended for users seeking interactive and real-time applications, such as chat and Web navigation, for example.[119] (EDMAN, SYVERSON, 2009; HOPPER, VASSERMAN, CHAN-TIN, 2010; MCCOY et al, 2008; CHAABANE, MANILS, KAAFAR, 2010; LI et al, 2010; AKHOONDI, YU, MADHYASTHA, 2012; ALSABAH, BAUER, GOLDBERG, 2012). This performance that seeks speed and interaction, however, comes at a cost: the network's resilience against certain types of attacks is diminished, meaning there is a reduction in the guarantee of anonymity. (EDMAN, SYVERSON, 2009; HOPPER, VASSERMAN, CHAN-TIN, 2010). More specifically, low-

[118] Although both use the onion routing technique, the TOR and I2P networks are different networks. On this, Li et al (2010) explains that "There are different variations of onion routers such as Tor, and Invisible Internet Project (I2P). These systems differ based on how the routing servers are organized; how the encryption algorithms are applied; how the tunnels are established; whether the transport-layer protocol uses TCP or UDP; or whether the clients relay traffic to other clients or not." (LI et al, 2010, p.8).

[119] This capability is possible because these networks actively seek to limit processing delay and bandwidth overhead. (HOPPER; VASSERMAN; CHAN-TIN, 2010, p.3).

latency networks are more susceptible to data traffic analysis by an adversary capable of observing the user's connection to the network and the network's connection to the destination intended by the user. (EDMAN; SYVERSON, 2009). In other words, while high-latency networks provide a strong degree of anonymity and degradation of the user's activity experience, low-latency networks offer precisely the opposite.

Another characteristic of low-latency networks is navigability using Web browsing "windows." This "window" is, in reality, the network's own browser and also allows file sharing, instant messaging, etc. – closely resembling the functionality of a conventional browser.[120] (MCCOY et al, 2008). The TOR network was especially concerned with user interactivity experience and achieved popularity, being the most widely used tool when it comes to anonymity technologies. (AKHOONDI, YU, MADHYASTHA, 2012; LI et al, 2010).

But delays also occur in the TOR network. Smaller than the delays of high-latency networks, but they exist and sometimes last seconds – which affects the quality of navigation, for example. (DUNGHEL et al, 2010). The main contributors to the delay are router-related delays – approximately 11% or more of the network's routers were overloaded with data traffic in 2010. And they are not the only ones contributing to the network's response delay. (Ibid., p.4). In fact, data traffic on the TOR network is not uniformly distributed among the various circuits.[121] A small number of circuits is responsible for consuming a disproportionate amount of bandwidth, and the greatest contributor is BitTorrent.[122] (ALSABAH; BAUER; GOLDBERG, 2012). Although Web navigation accounts for 92% of all TCP connections on the TOR network, this navigation accounts for only 60% of the volume of data traveling on the network. The other 40% of data volume is attributed to BitTorrent. (ALSABAH; BAUER; GOLDBERG, 2012). This means that BitTorrent is one of the most used protocols on the TOR network – which led Chaabane, Manils, and Kaafar (2010, p.174) to affirm that P2P ("peer-to-peer") traffic, such as BitTorrent, is not disappearing from the Internet but merely hiding in

[120] "The designers of the Tor network have placed a great deal of emphasis on achieving low latency and reasonable throughput in order to allow interactive applications, such as web browsing, to take place within the network." (MCCOY et al, 2008, p.67). That is, there was a political decision to reduce latency in order to achieve the objective of Web navigation within the TOR network. Web navigation is not encompassed by high-latency networks. The TOR network relies on an overlay, distributed network that uses "onion routing" technology to anonymize TCP layer applications (interactive applications such as browsing, data encapsulation, peer-to-peer communications). (CHAABANE, MANILS, KAAFAR, 2010).

[121] Circuits are the "paths" through which data travels within the TOR network, from sender to recipient. When data is sent, it does not circulate through all routers in the network: it travels along the circuit established between some of the routers. That is, within the universe of onion routers in the TOR network, the circuit is a pre-selected subset of them that provides the path through which data travels on the network.

[122] In 2010, it was believed that the volume of BitTorrent data traveling on the TOR network accounted for more than half, which caused damage to overall data traffic by forcing an increase in network latency and reducing speed. That is, the majority of data navigating the TOR network was encrypted BitTorrent data. (CHAABANE; MANILS; KAAFAR, 2010, p.170).

encrypted channels, such as within this anonymous network. In other words, BitTorrent is responsible for the degradation of the TOR network. On this, Johnson et al (2013) states:

> Our analysis shows that BitTorrent users not only degrade performance of the Tor network for everybody else, but against a Tor-relay adversary they get significantly less anonymity protection than typical users. [...] We observe that use of BitTorrent is particularly unsafe, and we show that long-lived ports bear a large security cost for their performance needs. (JOHNSON et al, 2013, p.337–347).

Users who use BitTorrent through the TOR network are also the "least" anonymous because their activities do not relate to Web navigation, like other users. This distinction in operations makes this group a "highlight" on the network, meaning they are more conspicuous. Therefore, besides being responsible for the degradation of the network, making it slower for users who use it for navigation, BitTorrent users are less protected than others. The constant improvements and implementations in the performance of the TOR network as a whole are essential for maintaining the degree of anonymity, navigation usability, and privacy protection of the users who compose this low-latency network. (ALSABAH; BAUER; GOLDBERG, 2012).

In terms of technical functioning, perhaps nothing is more important than understanding the TOR network system based on the principle of "three routers." In the literature on the subject, it is without a doubt the most widely described technical element. (DINGLEDINE, MATHEWSON, SYVERSON, 2004; DINGLEDINE, MATHEWSON, SYVERSON, 2007; MCCOY et al, 2008; PACHENKO, PIMENIDIS, RENNER, 2008; EDMAN, SYVERSON, 2009; CHAABANE, MANILS, KAAFAR, 2010; DUNGHEL et al, 2010; HOPPER, VASSERMAN, CHAN-TIN, 2010; LOESING, MURDOCH, DINGLEDINE, 2010; LI et al, 2011; AKHOONDI, YU, MADHYASTHA, 2012; ELAHI et al, 2012; FIFIELD et al, 2012; JOHNSON et al, 2013). This model of functioning based on the principle of three routers is also known as the principle of three nodes. At this point, it is important to remember how data packets travel through the mesh of the global computer network – as imagined and intended by Paul Baran, who was responsible for creating packet switching technology – because differences exist. And these differences in how packets travel and are transmitted are fundamental to understanding, at least partially, how anonymous networks are distinct regions of the global computer network.

The TOR network is composed of numerous unique servers called "onion routers" (Onion Routers, OR). (PACHENKO; PIMENIDIS; RENNER, 2008). These servers, or rather onion routers, are volunteer computers that form the network and are distributed in different locations around the world. It is from this ocean of volunteer computers that

any user creates a "path," also called a "circuit," through which their message will travel. This path is formed by nodes (volunteer computers). (EDMAN; SYVERSON, 2008).

The first step is to run an Onion Proxy (OP), which is nothing more than software that separates the local network from the external network.[123] (PACHENKO, PIMENIDIS, RENNER, 2008; DUNGHEL et al, 2010; LI et al, 2010; ELAHI et al, 2012). That is, this software is responsible for making the user's machine an integral part of the TOR low-latency anonymous network. The next step is to create a circuit from the available ORs – which are the volunteer computers that form the network. By default, the number of selected routers is three.[124] (MCCOY et al, 2008). Together, these three routers provide the path for sending and receiving data – and this is the circuit through which data is routed. The data is "encapsulated" according to the layered encryption strategy – typical of "onion routing" – and then travels the established circuit. (Ibid., p.64).

The network user initiates the session at the first node of the circuit. This first node is called the Entry Node. It is connected to the second node, called the Middle Node, through an encrypted tunnel established between the two nodes. Next, the Middle Node is connected to the third node, known as the Exit Node, also through an encrypted tunnel.[125] This encrypted tunnel resulting from the connection of these nodes is known as the "circuit" – the path through which encapsulated data travels. (EDMAN; SYVERSON, 2009, p.381; MCCOY et al, 2008, p.65). It is worth remembering that the default number of nodes is three but can be extended, as far as possible, by the user.

As stated earlier, messages are encrypted according to the typical "onion routing" scheme: the initial message is encrypted "n" times ("n" corresponds to the number of nodes in the circuit). If there are three nodes in the circuit, the message is encrypted three times, for example. The first layer of encryption can only be read by the last node, the Exit Node. This last node holds the cryptographic key to read the first layer. The penultimate node is capable of reading the second cryptographic layer. The antepenul-

[123]The definition of Proxy is as follows: "A proxy is a computer server or software program that is part of the gateway server or another computer that separates a local network from outside networks." (COMPUTER HOPE, 2017).

[124]"The default circuit length of three hops states a reasonable trade-off between security and performance. To avoid that the last node of a path (exit node) learns the first (entry node), an additional third node (middle node) is used." (PACHENKO; PIMENIDIS; RENNER, 2008, p.222). Typically the number of routers selected by the user is three, but nothing prevents the number from being different. These routers are also commonly called nodes. (EDMAN, SYVERSON, 2009; CHAABANE; MANILS, KAAFAR, 2010; DUNGHEL et al, 2010). If the user wishes a circuit with more than three routers, or nodes, they must download a list of them (with some additional information). In this list, there is an indication of the "status flag" of each available node (whose condition at the moment is considered by the user during their selection). The user chooses three active nodes (these are called "guards") that will serve as the gateway for the remaining circuits to be constructed. The "guards" are dynamically rotated over a period of 30 to 60 days – so as not to be static and easy "prey" for network adversaries. (JOHNSON et al, 2013, p.338).

[125]This third and final node is called the "exit node" because it is responsible for establishing a connection from the TOR network to the final destination intended by the user. (EDMAN; SYVERSON, 2009).

timate node is capable of reading the third cryptographic layer. And so on. This is the reason this cryptographic scheme is known as an "onion," as the message is wrapped in different layers and each node of the established circuit can only decipher a single layer of cryptography. For this reason, each intermediate node knows only about the node before and after itself – that is, no node is capable of recognizing all nodes in the circuit. (CHAABANE, MANILS, KAAFAR, 2010, p.167; AKHOONDI, YU, MADHYASTHA, 2012). In practice, each node of the circuit is capable of removing only a single layer of cryptography from the data packet and forwarding it to the next node. (DUNGHEL et al, 2010; HOPPER, VASSERMAN, CHAN-TIN, 2010; LOESING, MURDOCH, DINGLEDINE, 2010). Thus, only the entry node is capable of observing the originator of a specific request through the TOR network – in the same way that only the exit node is capable of identifying the message, removing the last cryptographic layer from the data packet, and knowing the final destination. That is, there is no way for a single router within the circuit to know the identities of the user and the recipient of the circuit, since each router knows only the "micro universe" composed of itself, its predecessor, and its successor. (MCCOY et al, 2008; DUNGHEL et al, 2010). The response, which travels from the final destination toward the network user, also uses the same onion routing cryptographic process: the message from the final destination is encrypted in layers and deciphered by the user. (LOESING; MURDOCH; DINGLEDINE, 2010). This data packet, the response from the final destination to the network user, is routed through the same three nodes as the original message – but in the reverse direction. (DUNGHEL et al, 2010). It is also worth remembering one detail: many users of the TOR network use the same intermediate nodes at the same time, so that the Internet connection of any one of these users is "hidden" among other connections of other users, which makes each individual system unfeasible to attribute to a specific user. (LI et al, 2011, p.2). For all of these reasons, the TOR low-latency network, which uses "onion routing" technology, is considered an anonymous network.[126]

The team that maintains the TOR network active, known as the Tor Project, developed a mechanism capable of circumventing actions by governments that seek to block connections to this anonymous network. This mechanism is known as "bridges." (LOESING; MURDOCH; DINGLEDINE, 2010). The problem originally occurs when Internet Service Providers (ISPs) companies responsible for connecting user devices to the global computer network, block access to the TOR network by filtering the IP addresses of the circuit's nodes. As a way to circumvent this blocking, the Tor Project created "bridges." It works as follows: when connecting their machine to the TOR net-

[126]One of the characteristics of the TOR network is the possibility of Web navigation through the browser of the same name, "TOR Browser." Instead of the nominal addresses of pages being listed with endings such as ".com" or ".org" or ".net," they are terminated with the suffix ".onion" – characteristic of TOR. Furthermore, this address is dynamic, changing with each visit request. (MOORE; RID, 2016, p.18).

work through the Onion Proxy, the user has the option to choose three nodes, or more, to create the circuit they will use. Node options are provided in a list of available routers (this list is in the "TOR Directory").[127] These "public" nodes of the TOR directory (since any user can have access) can be blocked by Internet service providers. Thus, those who wish to connect to the TOR anonymous network but find themselves, for some reason, blocked can request a "bridge" from the Tor Project. This "bridge" is an alternative means of access to the anonymous network (for those who cannot select nodes listed in the public directory). The Tor Project provides three "bridges" to the requesting user for a fixed period of time. Since these "bridges" are not listed in the public directory and exist for a limited time, it becomes difficult to locate them and consequently block them. (CHAABANE, MANILS, KAAFAR, 2010; LOESING, MURDOCH, DINGLEDINE, 2010). However, Moghaddam (2012) highlights the effectiveness of "bridges" while admitting that there are still ways to block them: since any user can request access to "bridges," it is possible to discover their IP addresses. Furthermore, censorship techniques undergo improvements and new implementations over time and, thus, new methods are deployed to discover and block these "bridges" offered by the Tor Project.

Still regarding possible "flaws" of the TOR network, which may, at some point, further reduce the degree of anonymity conferred by this low-latency network, Johnson et al (2013) reminds us that network users must make considerations about their own security needs – given that the network offers a lower degree of anonymity in exchange for greater usability and applicability (unlike high-latency networks). The risk of infiltration also exists: for example, a network user who has volunteered their machine to be an onion router with greater bandwidth. In 2013, Johnson et al conducted a study in which they found that there is a 50% probability of a user identifying others within an average period of up to 3 months. Within 6 months, this probability of identification rises to 80%. (JOHNSON et al, 2013, p.337). On this, Moore and Rid (2016) offer reassurance when they state that:

> Over time, civilian researchers and government agencies successfully de-anonymised some users, through methods ranging from planting compromised exit nodes that recorded traffic to employing malicious code within websites to covertly force users to access a public internet address controlled by the attacker, thereby revealing their true IP address. [...] But if a user employs even a fairly rudimentary set of cautionary procedures (such as keeping the browser up to date), the Tor core architecture remains relatively secure. (MOORE; RID, 2016, p.17).

[127]For more information about the TOR directory with the listing of nodes through the Onion Proxy, consult: EDMAN, SYVERSON, 2009, p.381; DUNGHEL et al, 2010, p.1; HOPPER, VASSERMAN, CHAN-TIN, 2010, p.5–6; LOESING, MURDOCH, DINGLEDINE, 2010, p.204; ALSABAH, BAUER, GOLDBERG, 2012, p.74–75; MOGHADDAM et al, 2012, p.97. To consult the technical functioning of the TOR network in more detail, especially regarding circuit creation, see ELAHI et al, 2012, p.43–45.

That is, despite the possibility of "de-anonymizing" the user, the careful implementation of some basic procedures provides the necessary robustness for the communication system to remain secure and protect the anonymity of users and the privacy of communications. The TOR software proves to be a relevant tool in the cyber domain, with adequate usability and functioning of reasonable comprehension by users who plan to use it as a Web navigation system and for other interactive communications.

Next, our objective is to describe the emergence of "hidden services" originating from the TOR network that, frequently, receive the name "darknet" for operating in the terms of a black market, with numerous products and services considered illicit, within the low-latency anonymous network. Without a doubt, the success of hidden services is due, to a large extent, to the robust use of cryptographic techniques – which led researchers Daniel Moore and Thomas Rid (2016) to consider the politics surrounding cryptography a relevant topic of academic discussion for the 21st century.

3.3.3 Hidden Services

The TOR software allows both anonymous navigation on the Surface Web and on the Dark Web.[128] The majority of users who use the TOR software do so to navigate the Surface Web in a more secure or anonymous manner.[129] (MOORE; RID, 2016). However, as we have seen, it is possible to interact within the network and access hidden pages at ".onion" addresses. From this logic arise the "hidden services" of the TOR network, as Moore and Rid (2016) attest:

> Tor, however, does not stop there. The network enables a far more controversial property as well. This capability, called a hidden service, allows anybody to create a virtually untraceable server hosted within the Tor network, simply by adding two short lines of code to a short configuration file. This allows circumvention of all known forms of content restrictions or surveillance. Neither the Internet Service Providers (ISPs) that route the traffic, nor law-enforcement agencies, nor even the developers of the Tor project itself have

[128] On the Tor Project page, on the surface web, it is possible to observe the listing of software and services offered by the project which, as of November 2017, included: "Tor Browser," a secure browser for Internet navigation; "Nyx," a terminal showing TOR network status; "Metrics Portal," analysis sciences of the TOR network; "Tor Messenger," an instant messaging platform operating on the TOR network; "Pluggable Transports," which transform data traffic of the TOR network between the user and the "bridge," in order to circumvent censors and blocks; "Onionoo," a Web-based protocol that provides information about TOR network routers and "bridges"; "Orbot," TOR platform on the Android operating system; "Shadow," a TOR network simulator; "Stem," a set of Python language terms for applications and programs that interact with TOR; "Tails," a system on USB drives pre-configured to use the TOR network and leave no traces on the local system; "Tor Birdy," a Mozilla Thunderbird extension; "Txtorcon," Python and Twisted implementations of the TOR control protocol; "Ooni," a global observation network. (TOR PROJECT, 2017).

[129] TOR software is a program that allows access to the anonymous network of the same name but that also offers other applications.

> visibility into the hosted service's location, or the identity of its operator. (MOORE; RID, 2016, p.17)

These Hidden Services are responsible for 3–6% of all TOR network traffic.[130] Research indicates that the most common use of these services is criminal in nature: involving everything from the drug trade to pornography involving children and animals. (Ibid., p.16). Moore and Rid (2016) also highlight the "fame" of TOR network hidden services in Russia: the powerful censorship organization, Russia's Safe Internet League, and press secretary and media regulator of the Kremlin, Vadim Ampelonsky, describe the TOR network as an environment that tolerates various illicit actions and allows criminals to hide from Russian authorities. Hidden services give a bad name to the TOR network and to cryptographic technologies in general. Curiously, despite being designed to leave no traces, none of the original creators mentioned illicit markets, a hidden service that emerged as a consequence of the network's system architecture and hidden pages. (Ibid., p.27).

In the face of cryptographic technology, the anonymous network, and hidden services, a myriad of actors emerges with the most diverse objectives: Islamic extremists, criminal communities, money laundering, drug and narcotics trade, child and animal pornography, hacking, violence, etc.[131] Some relevant points from the study by Moore and Rid (2016) are: the near-absence of Islamic extremist content in TOR network hidden services[132]; online criminal communities tend to migrate to the TOR network due to its security and anonymity features; money laundering is recurrent and the most used currency is Bitcoin; the most common commodity on the TOR network is drugs, of various types. If it is true that many criminal actions and illicit content find refuge in the low-latency anonymous network, then it is reasonable to suppose that there is growing difficulty for the discipline of Digital Forensics – which emerged as a field in the 1980s, with the first indications of virtual crimes, and has had notable prominence in the detection and prevention of digital crimes. (HORSMAN, 2017, p.448). In practice, evidence from Digital Forensics is used in courts of justice to support the criminal justice system. However, since 2010, the effectiveness of the discipline has been discussed while debating whether the golden age of Digital Forensics was coming to an end. Some affirm that there is sufficient evidence to state that this is true due to the great challenges faced by the field in light of the

[130]The term "darknet," employed by researchers Daniel Moore and Thomas Rid, for example, refers to this specific set of pages and services hidden through cryptography – as we saw earlier when discussing the definition of "Dark Web." (MOORE; RID, 2016, p.15).

[131]For more information, see "Appendix 6 – Classification."

[132]By all indications, there were some hidden network pages that were active in 2016, at the time of the research, but a small number. Extremists prefer to use the Internet in two ways: activities for the public (propaganda, recruitment, and sharing of suggestions) and activities hidden from the public (internal communication and command and control). (MOORE; RID, 2016, p.21). The Islamic State (ISIS) even has a page dedicated to propaganda on the TOR network's hidden service, launched in November 2015. (Ibid., p.29).

technologically cryptographic nature of many digital software and techniques. One such piece of evidence is the proliferation of anonymous digital markets originating from the hidden services of anonymous networks, such as TOR. (Ibid., p.449).

However, Roger Dingledine, one of TOR's creators, denies the relevance of "hidden services" within the network platform. (THOMSON, 2017). His criticisms revolve around the misinformation spread by journalists who, according to him, mix the network's "hidden services," which only 3% of users utilize, with simple anonymous Web navigation. According to Thomson (2017), for Dingledine, these hidden services (which he calls the Dark Web[133]) are insignificant.[134]

Originally, "hidden services" had their beginning in the 1990s with "BlackNet." Currently, hidden service networks use software to allow access to distributed networks, the greatest examples being the TOR, I2P, and Freenet networks. (MOORE; RID, 2016, p.7). In particular, the hidden services of the TOR network combine two specific characteristics, as Rid and Moore (2016) highlight:

> The first feature, hiding the physical location of all parties that are communicating, is a technical consequence of the onion-routing protocol – the trunk-sale effect. But the second feature, hiding the identity of the host, is a choice on the part of each individual service provider. Identities can be revealed, naturally, without losing the platform's security features, as one of Tor's most significant pioneers argues. (MOORE; RID, 2016, p.27).

In other words, the hidden services offered through servers are not specifically protected by the TOR network (although the communication and physical locations between agents who communicate through the network are), but rather by the Internet service providers, who possess the capability to determine at which address, within the mesh of the Internet, the server is located. In any case, the original creators of the TOR network acknowledge the network's hidden services and still seek adequate and appropriate uses for these services. (Ibid., p.29).

3.3.4 The Role of Cryptography

Perhaps the most curious fact is that cryptographic protocols, which underpin hidden services in general, were considered threats until around 1995. (MOORE; RID, 2016,

[133]Dingledine does not differentiate between the terms in the literature on the subject. In the mentioned context, it is evident that, for him, the "hidden services" of the TOR network and the "Dark Web" itself are the same thing.

[134]"Dingledine even went as far as saying the dark web – a landscape of websites concealed within networks like Tor – is so insignificant, it can be discounted. 'There is basically no dark web. It doesn't exist,' he told his DEF CON audience. 'It's only a very few webpages.' The most popular website visited by Tor users was Facebook, Dingledine said. In 2014 the ad giant embraced Tor, setting up a hidden service as a portal to its social network." (THOMSON, 2017).

p.28). In a cyber environment grounded in a culture of freedom and unfettered information flow, cryptographic protocols emerged as obstacles for third parties interested in the free communication between two agents. For this reason, Moore and Rid (2016) affirm that the politics surrounding cryptography is a crucial test of the values of 21st-century liberal democracy: while cryptographic power confers protection to citizens in their online shopping activities, reading, and banking access, this same power can protect malicious individuals. Cryptography is the central element of the greatest threats of our era – militant extremism and breaches in information systems – while simultaneously providing prosperity and privacy. (Ibid., p.7). This conflicting wave of positions regarding the politics around cryptography has been conventionally called the "Cryptowars," whose origin dates from the beginning of the 1990s with the debate surrounding the "Clipper" chip.[135] In sum, the "Cryptowars" are recurring and inconclusive technological debates about the government's position on accessing encrypted communications, or not, and involve national security actors, technology companies, and Internet users. (SCHULZE, 2017). Cryptography is the prominent element in debates involving the cyber domain and politics at the beginning of the 21st century. Furthermore, it is part of the central technical axis behind the TOR low-latency anonymous network – as we saw previously. For this reason, it is important to understand what cryptography is and what its properties are.

Cryptography is nothing more than a technique of "scrambling" legible text, using mathematical algorithms, into a ciphered and illegible text. (SCHULZE, 2017). Buchanan (2017) explains that "cryptography enables two parties to encrypt a message such that only the intended recipient can decrypt it. In a properly implemented cryptographic system, even if eavesdroppers intercept the message in its entirety, they cannot understand it." (BUCHANAN, 2017, p.4). That is, the objective of cryptography is to keep a given piece of information confidential from third parties, while perfectly comprehensible to the individuals intended to know the information. The problem, however, is the following: how can individual A, who enciphered the message using a given key, inform this key to individual B, who will use it to decipher the message? This question

[135]The beginning of the so-called "Cryptowars" was in 1992, when the American communications company American Telephone and Telegraph (AT&T) began developing a telephone capable of encrypting voice communication between two individuals. The proposal was the use of a chip called "Clipper" that would be attached to electronic equipment such as telephones and computers – and a copy of the encryption key would be stored in government databases. This key, in practice, allowed free government access. The debate continued until 1995, when the company's proposal was set aside. General Michael Hayden of the United States went so far as to state that the NSA lost this battle, affirming "We didn't get the Clipper Chip, we didn't get the back door." (SCHULZE, 2017, p.55). The debate was resumed in the new millennium, in 2014, when the technology company Apple decided to implement cryptographic standards in its cell phones, which generated a discussion involving the then FBI Director James B. Comey and Apple CEO Tim Cook. Both were at the center of the debate: while Comey insisted that the government adopt legislative measures on the subject of cryptography in technological devices, Cook argued that this action was excessively onerous. The debate continued until the following year when a Brooklyn court in the USA decided in favor of Apple. (Ibid., p.56). In summary, the debate is divided into two major voices: those who believe that cryptographic technologies are beneficial and those who claim the contrary. (Ibid., p.57; MOORE, RID, 2016, p.8).

is known as the "key-distribution problem." This problem is particularly serious in the military sector, going so far as to affect the tactical use of radio. (MOORE; RID, 2016, p.10). In 1976, the solution to the problem was unveiled: the solution was to adopt the "public-key" method. (SCHULZE, 2017). This is the milestone of modern cryptography. According to Buchanan (2017), "using a technology known as public-key encryption, it is possible to securely encrypt and transmit messages without any prearranged signals or codebooks." (BUCHANAN, 2017, p.4). The solution to the problem is to keep the key in public mode.[136]

For Moore and Rid (2016), the concept behind the public key was one of the pivotal inventions of the entire 20th century, as it allowed the recreation, and improvement, within the electronic context, of five fundamental properties of human communication: (1) privacy, a way to protect messages (especially in transit) against unauthorized access to content; (2) authentication, the way to identify that a message originates from a specific sender; (3) anonymity, the way to hide the identity of the author from both the recipient and other observers; (4) cash currency, which has no identity and is anonymous; (5) hidden exchanges, which is the possibility of carrying out exchanges and creating markets through which transactions are secure, authenticated, and anonymous. (MOORE; RID, 2016, p.11–14). The hidden services of anonymous networks recreate, with the help of cryptography, the environment for these spaces to proliferate: these hidden markets enable the exchange of goods and services, both licit and illicit, in an improved form – in the cyber domain. (Ibid., p.14). For the authors:

> All five cryptographically recreated properties – security, authentication, anonymity, digital currencies (to be more precise, 'blockchain' technology) and hidden exchanges – can be used or abused. Most forms of encryption have become a bedrock of the modern internet and the ubiquitous Public-Key Infrastructure, or PKI. (MOORE; RID, 2016, p.26).

Cryptography, currently, is part of a specific set of techniques that are embedded in the culture of the Internet. In particular, it has a relevant impact on the Dark Web, whether through the TOR low-latency anonymous network or through some other anonymous network such as Freenet and I2P. It should be noted, however, that the positions in the debate on the subject are broad: on one side, public actors who discuss the dangers arising from the use of cryptography in electronic equipment; on the other, private actors who extol the values of freedom, privacy, and security conferred by such mechanisms in

[136] "Authenticated key exchange (AKE) is one of the most important cryptographic constructs and is used to establish an authenticated and confidential communication channel. Existing approaches to two-party key exchange have emphasized mutual authentication, in which both parties authenticate themselves to their peer. [...] Other key exchange protocols aim to give anonymity, in which even the peer does not learn the long-term identity of the party. This is an important goal for practical applications such as the Tor anonymity network." (GOLDBERG; STEBILA; USTAOGLU, 2012, p.246–248).

the cyber domain. The so-called "Cryptowars" are recurrent and inconclusive events. The hidden services of the TOR network, despite not having been intentionally designed by their creators, are a phenomenon derived from the four properties of cryptography. (Ibid., p.28). For this reason, it has now become possible to make purchases and maintain private communications within the cyber domain in such a way as to remain hidden from the seller, tax authorities, law enforcement, or other third parties. (Ibid., p.14).

3.3.5 Popularity and Politics

It is said that the TOR network is the most widely employed anonymous communication system of the current era, becoming the most popular and widespread method. (PACHENKO, PIMENIDIS, RENNER, 2008; EDMAN, SYVERSON, 2009; DUNGHEL et al, 2010; LI et al, 2010; LI et al, 2011; ALSABAH, BAUER, GOLDBERG, 2012; ELAHI et al, 2012). The network gained some notoriety in 2004, when it had approximately 2,000 volunteer router nodes – reaching more than 250,000 nodes in 2009. (EDMAN; SYVERSON, 2009, p.380). This gain in terms of number of nodes is beneficial for the network because the more routers available, the more difficult it is to distinguish users when performing traffic analysis on the network. The increase in the number of routers increases the network's capacity to simultaneously manage users, in addition to decreasing the amount of traffic observed by an adversary who controls some of the nodes. (Ibid., p.388). One of the reasons for TOR's popularity is its anonymity implementation technique that combines parts of previous efficient methods, such as the router directory for user use, the establishment of telescopic circuits, and hidden locations. (LI et al, 2011, p.6). Furthermore, the TOR network has a more stable volunteer base than the I2P anonymous network – and in absolute terms, its number of volunteers is also larger. (Ibid., p.31). Anonymous networks, after all, are widely sought by users interested in privacy and anonymity. (CHAABANE; MANILS; KAAFAR, 2010).

If at the beginning the network's users were technical enthusiasts, as the project gained notoriety and recognition, new users with few technical skills began joining the network. The software was the subject of security conferences, technical journal articles, and traditional media outlets – such as the newspapers The New York Times and Wall Street Journal, and the American magazine Forbes. (DINGLEDINE; MATHEWSON, 2005). Indeed, the network is used by different social actors: from private citizens, through companies, to governments – and for reasons that range from the protection of virtual communications to the circumvention of censorship systems. (LOESING; MURDOCH; DINGLEDINE, 2010). It has also been considered a crucial service for government activists, journalists, enterprises, companies, and military sectors. (MITTAL et al, 2011, p.215). The more the network becomes popular among the masses, the more intense is the effort of governments to contain its use. The EFF has already positioned itself in favor

of the network, offering assistance to users of volunteer routers who received notifications from the American government through the Digital Millennium Copyright Act (DMCA) to remove their routers from the network. (MCCOY et al, 2008). Other actors who positioned themselves in favor of TOR include the giant Google and the organization Human Rights Watch, which advocates for navigation through the tool and recommends its use for dissidents, as a way to circumvent governmental repression measures. (MOORE; RID, 2016, p.17). In October 2017, The New York Times adopted the platform to offer its services.[137]

In 2008, the reach of the TOR network spanned approximately 126 countries, evidencing its global appeal – with prominence given to Germany, China, and the United States.[138] (MCCOY et al, 2008; LI et al, 2011). The anonymous network and the TOR project, ultimately, acquired distinctly political contours. In 2010, writing jointly with Loesing and Murdoch, one of TOR's creators, Roger Dingledine, admitted that the purpose of the TOR network is to offer anonymity and censorship circumvention for people around the world: "In particular, one goal is to make Tor more useful for people in various possibly censoring countries around the world." (LOESING; MURDOCH; DINGLEDINE, 2010, p.206). Chaabane, Manils, and Kaafar (2010) complement this, affirming that "historically, the main goal of these networks was to avoid 'political' censorship from a few countries and to allow freedom of speech on the Internet." (CHAABANE; MANILS; KAAFAR, 2010, p.167).

Indeed, the TOR network allows not only privacy in communications but also means to circumvent censorship imposed in some States and resist surveillance on the Internet. This aspect of the TOR network allows users residing in oppressive and/or authoritarian countries to have access to information without fear of reprisals such as blocking, tracking, or monitoring of their online activities.[139] (ALSABAH; BAUER; GOLDBERG, 2010). For example, if the user resides in an authoritarian country that mandates the censorship of Web pages, they can resort to the TOR network to circumvent this censorship and gain

[137]"The New York Times reports on stories all over the world, and our reporting is read by people around the world. Some readers choose to use Tor to access our journalism because they're technically blocked from accessing our website; or because they worry about local network monitoring; or because they care about online privacy; or simply because that is the method that they prefer. The Times is dedicated to delivering quality, independent journalism, and our engineering team is committed to making sure that readers can access our journalism securely. This is why we are exploring ways to improve the experience of readers who use Tor to access our website." (SANDVIK, 2017).

[138]It is important to understand where these data come from. On this, we highlight the literature of Finklea (2015): "Information is encrypted between relays, and 'all Tor traffic passes through at least three relays before it reaches its destination.' The final relay is called the exit relay, and the IP address of this relay is viewed as the source of the Tor traffic. When using Tor software, users' IP addresses remain hidden. As such, it appears that the connection to any given website 'is coming from the IP address of a Tor exit relay, which can be anywhere in the world'." (FINKLEA, 2015, p.4).

[139]According to Alsabah, Bauer, and Goldberg (2010), there is evidence of the TOR network's success: the number of software downloads and the growth of users on the network are indicative of its revolutionary character and its strength in the political and social struggle of these users' realities; being an influential anti-censorship technology.

access to the content of censored pages – they need only request the censored content and it will be delivered to them. (MOGHADDAM et al, 2012, p.97).

There are as many examples in the literature regarding the political use of the TOR network in different nations as there are of attempts to block its use by these same nations. The use of TOR in terms of number of users, for example, increased significantly in Iran's cyberspace from 2009 onward – after the Iranian elections. The TOR network is prominent in China and since September 2009 the Chinese government has blocked access to most of the network's onion routers.[140] For this reason, the number of "bridges," in the period following the blockage, increased by 70%. (LOESING; MURDOCH; DINGLEDINE, 2010, p.206). In Egypt, in 2011, thousands of individuals downloaded the TOR software for communication and dissemination of information – even after the strong Internet repression carried out by the Mubarak regime. Another highlight relates to the rebels of the Syrian conflict: they were able to expose digital evidence of the atrocities committed by the Bashar Al-Assad regime without exposing the identity of those who managed to gather the evidence. (MOORE; RID, 2016). Blocking attempts are made by Internet access providers at the local and regional level: since the list of the general directory of onion routers is open and public, blocking of the network can be done by blocking access to all routers on this list based on IP addresses (to locate them at their address within the Internet mesh). (MOGHADDAM et al, 2012). This is the reason why there exist routers outside of this listing – these are the "bridges."[141] However, it is worth remembering that "darknets" are not illegal in free countries. (MOORE; RID, 2016, p.32).

We conclude here the set of information about the TOR network necessary for understanding the reasons that make it a tool for combating censorship and a strong ally of user privacy.

3.4 The Knowledge Structure in the 21st Century

The global computer network became an important communication channel between individuals in the 21st century. Although she did not specifically address the cyber domain, Strange (1988) criticized specialists who claimed that the world was facing the "Information Revolution" without, at least, (1) pointing out what alterations this supposed revolution would make in the context of human relations, (2) or how it would displace

[140] This blocking phenomenon is linked to the policy of the "Great Firewall of China," which carries out censorship in the cyber domain. The onion routers have an IP number linked to the physical space of China. The IPs are relatively stable because they are listed in the standard TOR network directory, so that any user can choose routers from this list to build their own set of circuits – as explained previously.

[141] "Similarly, suggestions to require that entry and exit nodes for a given Tor circuit reside in different countries have been motivated at least as much by concern over attacks from administrative or governmental adversaries using legal or extralegal means as by concern about threats from the structure of the underlying communications network." (EDMAN; SYVERSON, 2009, p.388).

power, (3) or even how it could reallocate the efforts of human societies toward new goals. In fact, she agreed that at the end of the 1980s the world was making great technological leaps, partly supported by three major rapid changes: the development of quite sophisticated computer systems that allowed mass access due to low cost; the extension of these systems, including the use of satellites orbiting the Earth; and the digitization of language, bringing together different human groups previously separated by not speaking the same language. However, despite these technological changes being underway, her criticism resided in the fact that the majority of specialists of her era seemed only to explain what technology was doing and how it was operating. That is, they did not make political considerations about the element of power in the face of all these changes.[142] Those who ventured to make considerations about possible displacements of the locus of power, on account of the prevailing technological revolutions, diverged into two major groups: those who believed that the alteration of the locus was occurring and those who disagreed, believing that the locus remained unchanged. However, she herself did not position herself in either of these groups but pointed to the knowledge structure as an alternative, which should be considered alongside the others.

It is important to remember that Strange's initial reflections (1988) on the technological aspect at the end of the 20th century, in *States and Markets*, were based on a 1980s perspective. When she published *The Retreat of the State: The Diffusion of Power in the World Economy* in 1996, the Internet had already been commercialized – that is, part of human society was beginning to enter the environment of the cyber domain by navigating the Web for the first time, while the first companies that provided access to the cybernetic mesh of the global computer network were emerging. In 1996, the Internet was no longer isolated from the masses, almost restricted only to academic and military centers, used by computer scientists and enthusiasts – as was the case at the time of the 1988 publication. In the 1980s, indeed, the Internet was isolated from the general masses. Eight years later, Strange (1996) admits that the five principal changes[143] that occurred in the telecommunications sector, in market demands, and in political actions resulted in the displacement of authority from States to non-state actors. Previously, the State concentrated practically within itself the power to control knowledge and the means through which information circulated – by post offices, telegraphs, or telephones; in the 1990s, a set of actions enabled the opening of new options for communication channels for private companies and state governments. (STRANGE, 1996, p.100).

[142]Political in the sense that Strange (1996) uses, that is, not necessarily tied to the high echelons of government and politicians.

[143]According to Strange (1996), the five principal changes were: (1) improvement in information transmission systems (emergence of fiber optics, for example); (2) increase in the size of digital switches capable of serving a single large region or even a small country; (3) invention of telephones and cell phones that do not require wires, which drove the new market; (4) use of satellites orbiting the Earth; (5) more efficient transmission systems for computers and telephones that allowed the digitization of information, considerably reducing time and space between individuals.

As explained in previous sections of this chapter, the Internet is a hybrid dimension composed of physical infrastructure (cables, satellites, server computers, client computers, etc.) and digital abstraction (technology that allows data to traverse the network according to specific instructions, computer languages, byte compositions that result in digital files, protocols, the cyber domain, etc.). Strange's (1996) considerations about this new communication channel – produced from important technological alterations grounded in computer-based information systems, satellites, and fiber optic cables – seem to indicate that she was dealing, particularly, with the physical infrastructure of the global computer network. That is, she approached the thematic umbrella of telecommunications but did not enter the cyber topic. It is in the cyber domain that the existence of the TOR anonymous network, a component of the Dark Web, becomes relevant because, despite using the global computer network's infrastructure (physical) to function, it applies itself on the TCP/IP layer (abstract) to compose its operational channel.

Although she did not address the cyber aspect, we can make some observations based on the inputs provided by Strange herself when she discussed the knowledge structure, structural power, and the diffusion of power. According to her, and returning once more to the core of her discussion, the knowledge structure comprises (1) beliefs (including here the moral conclusions and principles that derive from belief); (2) all human knowledge, perceived and understood as such; and (3) the channels through which beliefs, ideas, and knowledge are communicated so as to allow communication – including the act of including some individuals and excluding others. Based on this, we can affirm that the TOR low-latency anonymous network is part of the knowledge structure for the following reasons.

First, the TOR network was conceived from very specific technical knowledge about computing that resulted in the implementation of "onion routing" technology. For this network to be formulated, it needed to be built, above all, upon the global computer network – which also derived from a set of very specific technical knowledge. The Internet, after all, was the result of different forces that first discovered unprecedented methods of applying knowledge – such as the case of Paul Baran (1964) and packet switching technology; Tim Berners-Lee, who developed protocols that culminated in the WWW; Marc Andreessen, who implemented graphics and images into browsers; among others. Thus, the Internet is the amalgam of the progress of constant ideas and implementation of innovative projects and knowledge that emerged at the end of the 20th century. And the TOR network?

Second, the TOR network was developed by members of civil society – Roger Dingledine and Nick Mathewson, both through the Free Haven Project – and a member of the American government – Paul Syverson, a member of the US Naval Research Laboratory. The technological design at the core of the anonymous network, and from which its name derives, is "onion routing." This design aims to implement anonymity in communica-

tions and also over the user's location within the Internet mesh (recalling that the TOR network uses the infrastructure of the global computer network). It should be recalled, as discussed in previous sections, that this design technique had been discussed since the beginning of the 1990s – which evidences the process of knowledge accumulation. Its creators classified the network they developed as being part of the third generation to use this technique. This point is relevant because it demonstrates, in practice, what was pointed out by Strange (1988) regarding knowledge: what is said to be known and perceived as understood is part of the knowledge structure. Therefore, the accumulated knowledge that enabled the creation of the TOR anonymous network, and upon which it relies to operate, is by definition part of the knowledge structure – given that this knowledge is perceived as understood and, moreover, shared around the world through undergraduate courses and educational centers on computing: it is the field of Computer Science, Information Systems, and Computing in general. If the knowledge structure comprises everything that is believed and perceived as understood, both the Internet and the TOR anonymous network are part of the knowledge structure – as defined by Strange (1988).

Third, the TOR network has become a relevant communication channel for sharing ideas, knowledge, and beliefs. It should be recalled that the Surface Web and the Dark Web – of which the TOR low-latency anonymous network is a part – are distinct regions of current cyberspace. The TOR network, despite using the Internet's infrastructure, is a network in itself and accessible only through the TOR software, designed specifically for navigating the network of the same name. Unlike the Internet, it is not an open network in the sense that it is accessible by any conventional browser, requiring only the typing of a domain name in the address bar. Managed by the Tor Project, the relevance of the TOR network is attributed to the anonymous character and the privacy it offers to users and the information exchanged through the network. And this relevance has been growing given the digital surveillance recently perpetrated by States and private companies on the Surface Web. (LANDAU, 2013; NOCETTI, 2015; LYON, 2015; MURATA, ADAMS, PALMA, 2017).

In particular, the TOR network assists those who, for some reason, find themselves at risk when using the Surface Web. This is the case for political dissidents, digital activists, human rights activists, journalists, whistleblowers, etc. (TOR PROJECT, 2018). A highlight is the non-profit organization Reporters Without Borders, founded in 1985 in France. This organization, of consultative status at the United Nations Educational, Scientific and Cultural Organization (UNESCO), at the Council of Europe, and a member of the International Organization of La Francophonie (OIF), is present in 130 countries through a network of correspondents. It has been disseminating in the journalistic community, through manuals, information about the functioning of the TOR network and the assistance it offers to professionals in the field regarding the shielding of communica-

tion and information exchanged – encouraging them to use it as their primary means of communication. (REPORTERS WITHOUT BORDERS, 2016). For Reporters Without Borders, the TOR network is an important tool for protecting dissidents and resisting censorship. (OVERLIER; SYVERSON, 2005). It is worth recalling that this organization is known worldwide for producing The Internet Censorship Ranking, in which it lists States according to the degree of censorship imposed on the network. (WARF, 2011). But Reporters Without Borders are not the only ones who use the TOR network as a relevant communication channel for carrying out their activities. At least two major widely circulated newspapers, The New York Times and The Guardian, offered a communication channel through the TOR network so that whistleblowers could share information with the editorial staff securely. (SANDVIK, 2018; THE GUARDIAN, 2018).

If the knowledge structure comprises the channels through which beliefs, ideas, and knowledge are communicated – as defined by Strange (1988) – it is reasonable to assume that, in general, the Internet is the most recent mass communication channel in use.[144] In this new communication channel, users (formerly known as "netizens") with access to the network are included, and those marginalized from it are excluded (whether due to lack of a computer, lack of a provider capable of connecting the machine to the global network, or any other circumstance that prevents the individual from entering the Internet mesh). Through the global computer network, through the implementation of different protocols, other communication channels operate in the "cyber" domain – as is the case with the TOR network. And just as the Internet in a general sense, the TOR network also enables the inclusion of some people and the exclusion of others on its network. The Internet and the TOR network are part of the knowledge structure, both being constituted from collaborative effort between civil society and the State for the development and creation of knowledge and tools of social relevance.

3.5 The TOR Network and Cyberpower

While Susan Strange confined herself to the treatment of power in the real geographical plane, Joseph Nye made considerations about the element of power in the cyber domain, indicating that this would be the "future of power" – indeed the title of his 2011 work, *The Future of Power*. There are at least four elements of discussion in Nye's work that are pertinent to this research and which we will briefly discuss: the diffusion of power; the knowledge structure; the definition of "cyberpower"; and the incidence of outcomes within and outside the cyber domain.

At first glance, readers may inquire about the similarities and differences regarding the phenomenon of the diffusion of power elaborated by Strange (1996) and Nye (2011).

[144]Especially if compared to other communication channels noted by Strange (1996): the system of telegraphs, post offices, and telephones [PPTs].

While the former discussed power diffusion as a qualitative deconcentration of power from the figure of the state, diluting into the international political-economic fabric toward non-state actors with sufficient authority and power to redefine others' options, the latter discussed the diffusion of power in the cyber domain. This diffusion of power, according to Nye (2011), was promoted by the reduction of entry costs for actors in the cyberspace region. Within this cyber region, actors use mechanisms and tools specific to this space to achieve desired outcomes. Both deal with distinct domains, the real plane and the cyber plane, yet both conclude that the diffusion of power concerns the displacement of concentrated power from the state figure toward non-state actors. Given the analysis of the database present in this research, we can conclude that there is, in fact, the emergence of non-state actors in the cyber domain who carry out operations in such a way that they achieve their desired objectives. Furthermore, we verified that these actors can be diverse – from researchers and cybersecurity specialists who act individually, to organizations concerned with maintaining the functioning of an anonymous network created by themselves and used by various other actors. The reduction of entry costs, as suggested by Nye and reflected in the dichotomy between technological improvement and price decrease, allows the presence of these individuals in the digital network based on microelectronics. These diverse actors are protagonists of the most distinct operations underway in the cyberspace region. In this sense, the State is not the sole actor with authority, control, or the capacity to alter the status quo – evidence of the diffusion of power underway. For Nye, in a world increasingly based on information, the diffusion of power and the emergence of non-state actors becomes a potentially more problematic threat than the transition of power between West and East, since the diffusion of power attests to the State's lack of control.

Regarding the knowledge structure, Nye does not explicitly use the IPE paradigm suggested by Strange based on four primary structures. However, it becomes clear that, at various moments in his work, he addresses the relevance of actors positioned within the knowledge structure or even the structure itself. For Nye, information occupies crucial power in this new era, affirming that "the spread of information means that power will be more widely distributed and informal networks will undercut the monopoly of traditional bureaucracy." (NYE, 2011, p.116). As is known, information/knowledge is the main element of the knowledge structure – which evidences that, indirectly, this structure occupies a prominent position in the new dynamics of power, according to the author's perspective.

Unlike Strange, Nye coined a definition for the power that operates in the cyber domain: "cyberpower." This power takes shape as it is defined through a set of resources related to computer-based information systems. Nye affirms that "cyberpower can be defined in terms of a set or resources that relate to the creation, control and communication of electronic and computer-based information – infrastructure, networks, software,

human skills." (NYE, 2011, p.123). One interpretation of this is that cyberpower is intimately involved with a set of resources related to the knowledge structure and the control dimension. Knowledge structure through the element of creation, which happens from the accumulation of knowledge about a given subject – in this case, knowledge based on computing. Control and communication relate to the knowledge structure insofar as control of communication channels provides a prominent position to those in their possession. And control dimension because it evidences the diffusion of power toward whoever possesses control over a relevant object for their purposes in the cyber domain. For Nye, "cyberpower is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyberdomain." (NYE, 2011, p.123). Cyberpower can be interpreted as an adaptation of relational power in the cyberspace domain. If we understand that obtaining preferred outcomes refers to the alteration of the status quo (in which the desired results had not been achieved), there are indications that the "cyberpower" defined by Nye operates in at least two dimensions: control and outcomes. Nye, however, considers that the alteration of the status quo can have consequences both within and outside cyberspace. He affirms that "cyberpower can be used to produce preferred outcomes within cyberspace, or it can use cyberinstruments to produce preferred outcomes in other domains outside cyberspace." (NYE, 2011, p.123). Although we agree that the alteration of the status quo can affect the cyberspace domain, we sought to address the consequences that affect geographical reality, for the purposes of this research.

3.6 Conclusion

The present chapter of this dissertation sought to address matters related to the history and functioning of the Internet, the classification of the Dark Web in the context of the WWW, and the specific technologies of the TOR anonymous network. From this, the so-called "hidden services" of the Dark Web, the political role of cryptography, and the popularity of the TOR anonymous network were discussed. Finally, we sought to establish the TOR anonymous network as a relevant part of the knowledge structure in the 21st century.

Initially, we sought to ground the reasons why we believe the TOR anonymous network falls within the knowledge structure – a conceptual element defined by Strange (1988) at the end of the 1980s. Although she did not explicitly address the Internet, Strange (1996) highlighted the relevance of information systems, the use of satellites, and the technology developed by computing in human communications. Our analysis focused on a specific region of cyberspace that is the product of accumulated knowledge gathered primarily by individuals from civil society – although, in the case of the TOR network, there was the presence of a member of the public sector in the origin of the network's

development.[145] As a final element presented, we highlighted some considerations about the TOR anonymous network and the "cyberpower" defined by Nye (2011).

We believe that the content addressed in this chapter is relevant and necessary for the analysis of power diffusion in the following chapter. Thus, in the next chapter, we will address the journalistic articles from which the non-state actors that participated in our analysis originated. We present, finally, the results of the diffusion of power in three dimensions for thematic groups individually and compared among themselves. Furthermore, we will present the diffusion of power in a general manner across all occurrences.

[145]Specifically a member of the US Naval Research Laboratory.

Chapter 4

Analysis of the Diffusion of Power in the Tor Network in Three Dimensions

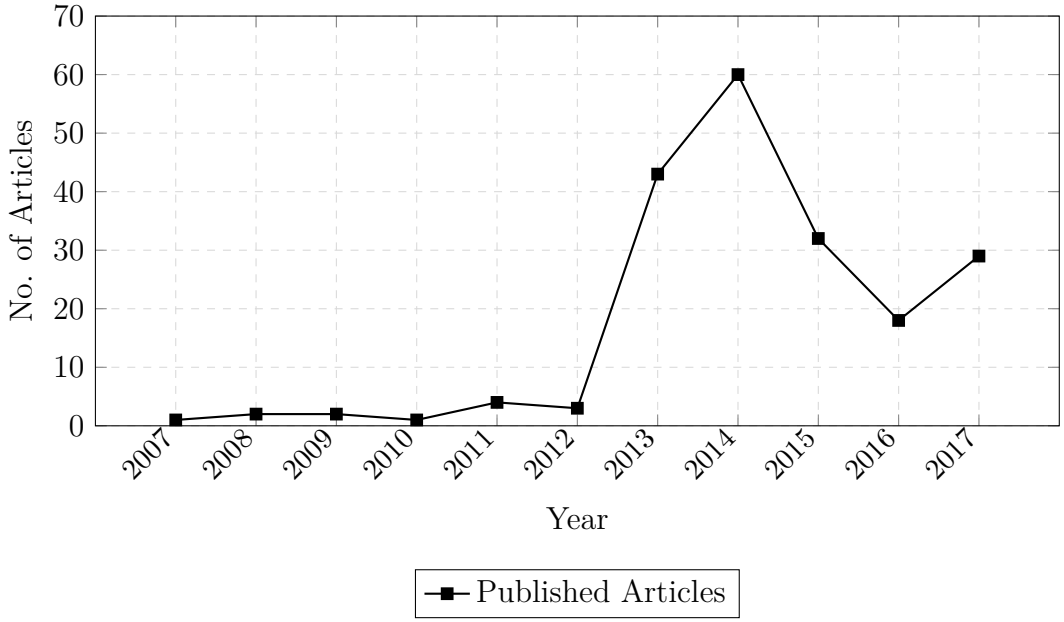
The third chapter of this dissertation aims to present the analyses of diffusion of power in three dimensions carried out from a database composed of information derived from journalistic articles. The database presents the variables "authority," "control," and "outcomes" that emerge from the operationalization of the three dimensions of the same name. In order to provide context for the variables, we also identified other relevant information such as the identification of peers and stakeholders (relative to the authority dimension), the object considered relevant for achieving the desired outcome by the non-state actor in the context of the article (relative to the control dimension), and the effect on reality (relative to the "outcomes" dimension). In addition, the database is composed of other information related to the identification of the newspaper articles such as authors, newspapers, country of headquarters, article title, etc.

The analysis was conducted according to the methodology defined in the Introduction of this dissertation and uses the operationalization of the phenomenon of diffusion of power – based on the frequency of occurrences of each variable, which allowed us to generate statistical tables. For the purposes of this dissertation, from the readings of the articles we identified non-state actors and grouped them according to themes common to them. From this, we will present the results of the diffusion of power analysis in three dimensions – authority, control, and outcomes: for each dimension, the results of (a) the individual analysis of each thematic group, (b) the comparative analysis between thematic groups, and (c) the general analysis of total occurrences were presented. The charts, tables, and figures that emerged from the interpretation of the data, together with the database of 139 occurrences, can be found in the appendix of this dissertation.

4.1 Journalistic Frequency Regarding the Tor Network

In order to understand the publicity given by these newspapers to the topic of the anonymous network, we examined the number of articles published per year and, thus, obtained the following chart.

Chart 1 – Number of Articles Related to "Tor Network" Published Per Year (2007–2017)



Source: Author.

The 195 articles were distributed over a period of one decade, as shown above. From this chart, we can make some observations regarding the average number of articles published prior to 2013, the growth in the number of publications in 2013–2014 and 2017, and the change in level after 2014.

Initially, between the years 2007 and 2012, we observed few articles published by the aforementioned newspapers – 13 articles in total. This average changes in the following years. In 2013, the number of published articles surpassed the mark of 40. Three subjects were mainly responsible for this increase: (1) the activist organization Tor Project, responsible for the maintenance, improvement, and operationalization of the anonymous network, was cited throughout the news stories that highlighted the Tor network itself or the topic of the Dark Web; (2) the anonymous online marketplace Silk Road, whose main administrator, Ross Ulbricht, was imprisoned by North American authorities in October 2013; (3) and the revelations of Edward Snowden, which exposed the global surveillance scheme perpetrated by the US government and its allies.[146]

[146]See "Appendix 5 – Articles Published in 2013."

In 2014, the number of publications reached the level of 60 articles – 50% more than the previous year. In addition to the subjects mentioned earlier, three others also contributed to the increase: (a) the rise of the online marketplace Silk Road 2.0, which sought to continue the previous version closed in 2013 by US law enforcement authorities; (b) the operation of transnational child pornography networks through the anonymous network; (c) and the exposure of the topic of privacy and anonymity on the Internet.[147]

While in the period of 2013 and 2014 there was growth in the number of published articles related to the Tor anonymous network, in the following years a decrease in the number of these publications occurred. Only in 2017 was there a slight increase. It is relevant to note that after 2014, publications related to the Tor anonymous network shifted to a higher level compared to the period before 2013: previously they did not reach 10 publications per year, and afterward they published no fewer than 15 news articles. This change in level reflects the interest of journalistic coverage in, primarily, the so-called "anonymous markets" of the Dark Web. These markets are known especially for trading drugs, narcotics, and other illicit substances. In 2017, for example, the Alphabay marketplace dominated journalistic publications involving the Tor anonymous network. But the change in level also reflects the journalistic coverage given to the arrests of administrators and those responsible for child pornography networks by police authorities of various governments.[148]

During this ten-year period, the British newspapers The Guardian and Mail Online and the American newspaper The Washington Post were those that produced the most news articles related to the Tor anonymous network. The Eastern newspapers, Tribune Newspaper, People's Daily Online, and Xinhua News Agency, were those that gave the least publicity to the topic.

[147]See "Appendix 6 – Articles Published in 2014."
[148]See "Appendix 7 – Articles Published in 2017."

Table 4.1: Number of Articles Related to "Tor Network" Published by Each Newspaper (2007–2017)

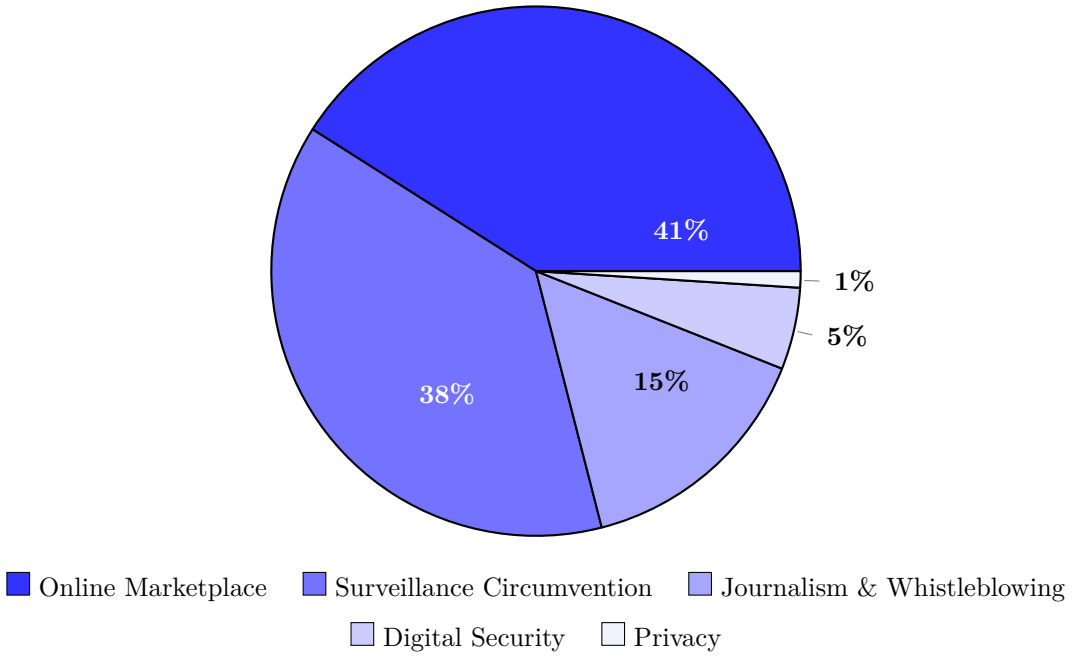
Country	Newspaper	N
England	The Guardian	64
England	Mail Online*	53
USA	Washington Post	31
England	Telegraph Media Group	17
USA	Advance Digital**	17
USA	The NY Times	11
India	Tribune Newspapers	1
China	People's Daily Online	1
USA	Hearst Newspapers	0
China	Xinhua News Agency	–
	Total	**195**

4.1.1 Actors and Thematic Groups Derived from Journalistic Articles

From the elaboration of the database, we identified 26 actors derived from 139 occurrences (these originating from 125 newspaper articles). These actors were allocated into 5 categories formulated by us that correspond to distinct thematic groups. This classification was elaborated from the reading of the 125 newspaper articles.

The first thematic group, **Digital Security**, comprises actors related to information and network security: Dan Egerstad; Freedom Hosting; Iranian Cyber Army; Onion Ransomware; Ransomware; SimpleLocker Android Malware; Carnegie Mellon University. The second thematic group, **Surveillance Circumvention**, encompasses actors that, in some way, "circumvent" digital surveillance perpetrated primarily by state actors: Tor Project and Facebook. The third group, **Online Marketplace**, is composed of anonymous online marketplaces that operate on the Tor network: Silk Road; Silk Road 2.0; Silk Road 3.0; Alphabay; Farmer's Market; Evolution and Sheep Marketplace. The fourth thematic group, **Journalism & Whistleblowing**, comprises actors engaged in the disclosure of confidential information or involved with the journalism profession: Edward Snowden; WikiLeaks; SecureDrop System; Strongbox; ProPublica; Harold T. Martin; Chelsea Manning and X-Net Group. And, finally, the group **Privacy** involves actors that, in some way, are related to data exposure and the privacy of individuals: Doxbin.

Chart 2 – (%) Occurrences by Thematic Group (2007–2017)



Source: Author.

The group that appeared most frequently in newspaper articles, in percentage terms, was the Online Marketplace group, with 41% of occurrences concerning actors involved in the commercialization of illicit products, services, and goods on the Tor anonymous network. Next came the Surveillance Circumvention group, with 38% of occurrences reporting actions of the actors that compose this group. The highlight is given to the actor Tor Project, responsible for the maintenance of the Tor anonymous network, improvements, and digital activism. In third place, the Journalism & Whistleblowing group, with 15% of occurrences exposing actions of actors who deal with journalism or are, in some way, involved with disclosures. Finally, the Digital Security group, with 5%, and in last place the Privacy group, with 1% of occurrences.

The first thematic group, Digital Security, comprises six actors related to the technical security of information and networks in general.

The security researcher, **Dan Egerstad**, aged 21, was responsible for finding security flaws in the communications of various embassies such as Russia and India. According to Kirk (2007), Egerstad managed to download confidential files. The embassies used the Tor network with the objective of protecting their communications but, as pointed out by Egerstad, they failed to protect the entry and exit nodes of the Tor network with encryption. It is worth remembering that the central nodes of the tunnels created by Tor are automatically encrypted – but not the entry and exit nodes, which require the user to manually protect them with a cryptographic layer. (KIRK, 2007). The knowledge of the young security researcher enabled the discovery of relevant flaws in communication

between the embassies, as well as their remediation.

The **Iranian Cyber Army** is a group that carries out activities in the cyber domain and works alongside the Iranian government. (CUBRILOVIC, 2009). According to the news story written by Cubrilovic (2009), the group launched attacks on the servers responsible for hosting Twitter's DNS records. With access to the Twitter account, the Iranian Cyber Army altered the DNS records of the address "twitter.com" so that, instead of redirecting to the standard server, they pointed to a specific IP address on the Tor anonymous network. This attack coincided with the escalation of diplomatic hostility between Iran and the USA, as well as the incursion of Iranian troops near oil dispute borders. (CUBRILOVIC, 2009).

The next three actors – **Onion Ransomware**, **SimpleLocker Android Malware**, and **Ransomware** – are software programs, developed by an individual or group of individuals, whose objective is the "hijacking" of certain files or functionalities of user devices. Files and functionalities are returned only upon payment of monetary sums. This type of software is known in the literature as "ransomware." (GAZET, 2014; SCAIFE et al, 2016). Of these three ransomwares mentioned above, the first one, "SimpleLocker Android Malware," was reported in June 2014 by Tom Brewster. According to the journalist, this ransomware attacked devices using the "Android" operating system by scanning the memory of the devices to encrypt certain files and, thus, demand payment from the user for data recovery. The files hijacked by this ransomware were sent to servers within the Tor network. (BREWSTER, 2014). The second of these ransomwares, "Onion Ransomware," was reported in July 2014 by Alex Hern. According to the journalist, this ransomware was responsible for hijacking files from user devices, using the Tor network to keep its technical nature and activities hidden. Once the device was infected with the "Onion,"[149] it displayed a screen with a 72-hour countdown timer. If payment was not made within this period, the files were discarded. (HERN, 2014). The third ransomware, described by Charles Arthur in 2017 simply as "Ransomware," attacked various hospitals in the United Kingdom. As usual, it demanded the payment of monetary sums for the recovery of data and files. But the payment, in this case, was to be made through the cryptographic digital currency "Bitcoin" to a page hosted on the Tor network. (ARTHUR, 2017).

The last actor in this category is the server **Freedom Hosting**. This server, in 2013, was considered the largest on the Tor anonymous network – and was generally associated with illicit content. (PETERSON, 2013). In 2013, it was infected by a "malware" that is believed to have been implanted by the Federal Bureau of Investigation (FBI) with the objective of taking it out of operation. To achieve this, the malware exploited a security

[149]Not to be confused with The Onion Router (Tor) or the technical design known as "Onion Routing." In this case, "Onion" is merely the name of this specific ransomware.

breach in older versions of the conventional "Firefox" browser[150] to implant itself in the Freedom Hosting server and use its own code developed for the identification of users who accessed the server. It is noteworthy that the breach was found in the Firefox browser – that is, there was no security breach in the Tor network itself. (PETERSON, 2013).

The American university **Carnegie Mellon University** is a private institution in the education sector, headquartered in Pennsylvania, USA. According to Alex Hern (2016), the US Department of Defense funded research at Carnegie Mellon University with the objective of discovering tactics that could remove the "anonymity" of Tor network users. The Tor Project organization identified, at the beginning of May 2014, that some nodes of the anonymous network appeared to be directing their efforts toward identifying other nodes and, for this reason, were removed from the network in June of the same year. The following month, in July 2014, researchers at Carnegie Mellon cancelled the public presentation of a paper whose content sought to reveal tactics for identifying the IP addresses of Tor network users. Hern (2016) points out that documents released by the court in the Silk Road case confirmed the involvement of Carnegie Mellon University in the identification of anonymous network nodes, and the information collected was accessed by the FBI. (HERN, 2016).

The second thematic group, "Surveillance Circumvention," highlights two actors that offer means to circumvent digital surveillance: the Tor Project, through the anonymous network of the same name, and Facebook, which is the first social media platform to offer access through the low-latency network.

The non-profit organization **Tor Project**, responsible for managing the Tor anonymous network, is intimately related to the provision of methods that circumvent digital surveillance, especially perpetrated by some countries in the form of censorship. According to Vitaliev (2008), Bradbury (2008), and Anderson (2009), the Tor Project offered an alternative means of Internet access to users residing in China and Iran, countries recognized for maintaining strict censorship over various content available on the Internet. China is known for using a "firewall" system to filter content and restrict the access of Chinese citizens and residents, which became known in the literature as "The Great Firewall of China." (CLAYTON, MURDOCH, WATSON, 2006; ANDERSON, 2012; ENSAFI et al, 2015). The government of Iran, in turn, became known for controlling exit "gateways" – especially in moments preceding elections and during popular unrest. (ANDERSON, 2009). The Tor Project is known for providing "Tor Bridges"[151] to users who intend to circumvent censorship and freely use Internet access through the Tor network.

The **Facebook** platform began as a private network for Harvard University students launched in February 2004 on the Surface Web. Currently, Facebook is a private company

[150]The "Firefox" company opted to incorporate into its browser features from the Tor browser itself to increase the privacy of its users.

[151]More about "Tor Bridges" was discussed in Chapter 2.

headquartered in California and widely used on the Surface Web by users from various countries. In October 2014, according to Fox-Brewster (2014), the social media service opened an address on the Tor network, offering an access channel to users who navigate through the anonymous network. The objective is not to provide anonymity to users who access the service through Tor – since they access identity profiles when they log into the Facebook service – but rather to circumvent censorship in authoritarian regions and digital surveillance carried out by local entities, as well as to offer additional layers of connection protection. (MOYER, 2014).

The third thematic group, "Online Marketplace," encompasses seven online markets that operate, or operated, on the Tor network and were popularly known among users as "black markets of the network" and publicized on Surface Web news sites. Martin (2013) proposes treating anonymous online markets as part of a new concept of cybercrime – "cryptomarket" – whose intention is to highlight this emerging area of specific crimes. According to the author, "a cryptomarket may be defined as an online forum where goods and services are exchanged between parties who use digital encryption to conceal their identities."[152] (Ibid., p.356). The types of goods and services traded in "cryptomarkets," especially the illegal trade of drugs, justify the treatment of these markets as part of the concept of cybercrimes. In any case, the literature on the subject emphasizes the modernity of the phenomenon of anonymous online markets and the challenge they present to law enforcement.[153] (BARRATT, LENTON, ALLEN, 2012; CHRISTIN, 2013; MARTIN, 2013; RON, SHAMIR, 2014; VAN HOUT, BINGHAM, 2014).

The first of these markets, and the most well-known and widely discussed in the literature, is the online marketplace **Silk Road** – launched in February 2011, as a hidden service of the low-latency Tor network, and shut down by the FBI on October 2, 2013. (CHRISTIN, 2013; BIRYUKOV, PUSTOGAROV, WEINMANN, 2014; BRADBURY, 2014; RON, SHAMIR, 2014; VAN HOUT; BINGHAM, 2014; MADDOX et al, 2015). Its name alludes to the ancient Silk Road, a trade network that connected the European, African, and Asian continents.[154] (PHELPS; WATTS, 2014). It became known as an

[152]Some encrypted online markets are considered by the literature. Martin (2013), for example, defines what an ideal market of this type would be: "Ideal type cryptomarkets may also share the following characteristics: reliance on the Tor network; use of cryptonyms to conceal user identity; use of traditional postal systems to deliver goods; third-party hosting and administration; decentralized exchange networks; use of encrypted electronic currency (e.g. Bitcoin)." (MARTIN, 2013, p.356). Maddox et al (2015) observe "cryptomarkets" as a "digital demimonde," that is, an isolated and marginalized world from everyday life that operates on the "fringes of the publically accessible Internet (through Tor) and social mores." (MADDOX et al, 2015, p.111–112).

[153]The anonymous character is conferred through the use, also, of cryptographic digital currency to make payments – such as, for example, the Bitcoin currency. (BARRATT; LENTON; ALLEN, 2012, p.6).

[154]"Silk Road moderators explained the websites name and beginnings: 'The original Silk Road was an old world trade network that connected Asia, Africa and Europe. It played a huge role in connecting the economies and cultures of those continents and promoted peace and prosperity through trade agreements. It is my hope that this modern Silk Road can do the same thing, by providing a framework for trading partners to come together for mutual gain in a safe and secure way'." (PHELPS; WATTS, 2014, p.5).

encrypted marketplace specializing in the illegal trade of drugs. (MADDOX et al, 2015). According to Christin (2013, p.8), the 4 most popular categories[155] of the market are related to drugs, while 6 categories in the "top 10" and 16 categories in the "top 20" are related to narcotics and drugs. Thus, despite not exclusively trading drugs, the marketplace predominantly dealt with the commerce of narcotics – offered by various different vendors.[156] Drugs were traded, above all, in small quantities so as to serve the interests of users.[157] (MARTIN, 2013). For these reasons, in addition to presenting a user-friendly online shopping interface, the Silk Road marketplace became known as the "E-Bay of Drugs." (VAN HOUT; BINGHAM, 2014; MARTIN, 2013; PHELPS, WATTS, 2014; MASONI, GUELFI, GENSINI, 2016).

The administration of Silk Road was carried out by one person, whose identity remained unknown during its operation, who called himself "Dread Pirate Roberts" (DPR) and who controlled all aspects of operations.[158] (RON; SHAMIR, 2014). When the marketplace was shut down by law enforcement, his identity was revealed: he was the American citizen Ross Ulbricht – who at the time of his capture was 29 years old. (BRADBURY, 2014). According to the documentary "Deep Web," 2015, directed by Alex Winter, which recounts the journey of Ross Ulbricht, during the creation of the black market, the young American left clues about his identity on the Surface Web – such as his personal email address on online communication forums. The closure of the marketplace was considered the first significant act by law enforcement in disrupting the environment of a cryptographic online market and occurred in October 2013. (MADDOX et al, 2015, p.122). However, shortly after this event, other cryptographic online markets dedicated to anonymous transactions emerged, such as Silk Road 2.0, "Atlantis," and "Agora."[159]

[155]Christin (2013) conducted a study that tracked the anonymous Silk Road marketplace between the period of February 3, 2012 and July 24, 2012, and during this period was able to verify the volume of 24,385 items (unique, that is, not repeated) being traded. The market distinguished around 220 different product categories ranging from digital products to narcotics and prescription medications.

[156]Corroborating this view are Biryukov, Pustogarov, and Weinmann (2013): "Silk Road is a market that operates mostly in contraband goods using Bitcoin as currency. According to a recent study primarily narcotics and other controlled substances are sold on this platform." (BIRYUKOV; PUSTOGAROV; WEINMANN, 2013, p.81).

[157][...] "most transactions conducted via Silk Road are for purchases of relatively small amounts of illicit drugs. This means that the volume of drugs which most buyers receive is relatively small and (depending on jurisdiction) would likely constitute a lower-level drug possession rather than commercial trafficking charge." (MARTIN, 2013, p.360–361). Regarding the economic impact, Martin (2013, p.353) states that, while the American trade generated approximately 300 billion US dollars in 2005, the Silk Road corresponded to a smaller trade of approximately 23 million US dollars in the same year.

[158]Phelps and Watts (2014, p.2) point out that the identity behind the pseudonym "Dread Pirate Roberts" cannot be confirmed as belonging to a single person. Probably, the difficulty in confirming the exclusivity of the pseudonym solely to Ulbricht occurs due to the origin of the pseudonym itself – in the film "Princess Bride," 1987, directed by Rob Reiner, "Dread Pirate Roberts" was the pseudonym used by various characters who performed the same role across generations.

[159]On this topic, Lacson and Jones (2016) argue that the end of the popular market does not mean the interruption, or the end, of the Dark Web environment – since its ending can be interpreted as part of a continuous narrative, and of the development, of the Dark Web's black markets. Christin (2013, p.2) further notes the existence of other anonymous online markets such as "Black Market Reloaded," "The

(BERGHEL, 2017).

The closure of the online black market Silk Road did not indicate the end of online markets that operate services on the Tor network. (POWER, 2013). In fact, in the month following the closure of the Silk Road by the FBI and DEA, the second version of the black market emerged: **Silk Road 2.0** – whose intention was to continue the Silk Road brand under new leadership. (DEMANT; MUNKSGAARD; HOUBORG, 2016). According to Demant, Munksgaard, and Houborg (2016), in the period between November 2014 and April 2015, the Silk Road 2.0 marketplace traded approximately 66 million US dollars – Cannabis was the best-selling product. The marketplace was managed by Blake Benthall, a 26-year-old American resident of California, a software engineer in Silicon Valley – more precisely, he worked for Elon Musk's company "SpaceX." (ASSOCIATED PRESS; PRIGG, 2014). One year after its opening, Blake Benthall was arrested by American law enforcement during an international operation orchestrated by different countries, "Operation Onymous," with the involvement of Europol and whose objective was to deter crimes related to drug trafficking conducted in the cyber domain. Law enforcement agents infiltrated the black market, gaining trust and receiving compensation to administer certain sections of Silk Road 2.0 – which gave them access to privileged information. (FOX-BREWSTER, 2014; RUSHE, 2014).

Again, in November 2014, following the closure of the online marketplace Silk Road 2.0, the **Silk Road 3.0 Reloaded** marketplace appeared on the Tor anonymous network – continuing the Silk Road brand. (ASSOCIATED PRESS, 2014).

Another influential black market on the Tor network was the **Sheep Marketplace**, which emerged shortly after the closure of the first Silk Road and was "invaded" by vendors and consumers seeking an alternative marketplace to continue their commercial transactions. (GARDNER, 2013). This black market also traded various products, among which drugs and weapons were the main ones. Like the Silk Road, the Sheep Marketplace conducted financial transactions in Bitcoin, and also adopted the payment mechanism known as "escrow."[160] However, shortly after receiving a large volume of orphaned users from Silk Road, the Sheep Marketplace closed its doors, taking with it large quantities of Bitcoin from users registered on the marketplace – which raised suspicions

Armory," and "The General Store."

[160]This system was characteristic of the Silk Road marketplace. Its objective was to provide some degree of trust in financial transactions between buyers and sellers – since both are anonymous in the black market. According to Bradbury (2014), its functioning was as follows: "Customers would send their payment in bitcoins to an electronic address operated by Ulbricht, who also employed several administrators. Silk Road would then act as an escrow service, holding the funds until the customer confirmed that they had received the goods. The service would then release the money after taking a commission." (BRADBURY, 2014, p.15). Phelps and Watts (2014) complement, stating that the system "Escrow provided users with a level of security from potential fraudulent transactions in the marketplace. The Bitcoins were held in an account managed by Silk Road administrators and once the item had been shipped by the seller Silk Road would remove a predetermined amount of commission and finalise the purchase by releasing the remaining funds to the seller." (PHELPS; WATTS, 2014, p.3)

that, in reality, it was a scheme to seize Bitcoins. (GARDNER, 2013).

The **Farmer's Market** black market also operated on the Tor anonymous network, but, unlike the others, accepted other forms of payment that were not in the cryptographic digital currency Bitcoin – such as cash and transactions via Paypal and Western Union. (ASSOCIATED PRESS, 2012). This marketplace was managed by eight men of different nationalities who, together, promoted the meeting between drug suppliers – such as LSD, Ecstasy, and Ketamine – and potential consumers through the online marketplace. Law enforcement from the USA, Colombia, the Netherlands, and Scotland worked together in "Operation Adam Bomb," whose objective was to arrest the eight individuals – and they carried out this activity successfully. (ASSOCIATED PRESS, 2012). In this same vein, the **Evolution** marketplace also acted, which also saw its number of users grow after the capture of Ross Ulbricht, the administrator of Silk Road best known by the alias "Dread Pirate Roberts." This marketplace, which also served as a meeting point between sellers and buyers of illicit merchandise, likewise disappeared from the Tor anonymous network, but not before taking with it large sums of Bitcoins held in the marketplace's "escrow" system. (FARRELL, 2015). This "disappearance" from the network led researcher Henry Farrell (2015) to conclude that, in order to eradicate black markets from the Dark Web, it suffices for law enforcement to make an impact by apprehending a sufficient number of administrators behind the marketplaces so that the others ponder the long-term future of the marketplace and desist from operating criminally on the network.

Finally, the last online black market of the Tor anonymous network to appear in the newspaper articles that compose the database of this research is the **AlphaBay** marketplace. Similar to the others, this marketplace also enabled the commercial transaction of various illicit substances and diverse services. Moreover, it was one of the marketplaces with the longest active operating time – from December 2014 to July 2017. (TZANETAKIS, 2018). It is estimated that the "Stimulants" category, such as cocaine, represented 20.98% of the substances traded on the marketplace – followed by the "Cannabis & Hashish" category, with 18.47%, "Opioids," 12.69%, and "Ecstasy" fourth, with 11.69%. (TZANETAKIS, 2018). While active, the AlphaBay marketplace was considered one of the largest online drug markets, in terms of number of products and page users – providing a highly competitive environment. (PAQUET-CLOUSTON; HETU; MORSELLI, 2018). On the AlphaBay marketplace, sellers were required to pay a registration fee that cost around 200 US dollars – a value considered low for entry into the digital market. (Ibid., p.95). In July 2017, AlphaBay was shut down by law enforcement coordinated by different agencies across various countries. (TZANETAKIS, 2018).

The fourth thematic group of this research, "Journalism & Whistleblowing," encompasses eight actors who are in some way related to journalism activities or disclosures of corporate and/or governmental schemes or secrets. Some of them are quite well known to the general public.

The non-profit organization **WikiLeaks** gained notoriety in 2010 after the disclosure of confidential information from American embassies, coordinating with five other major globally circulated newspapers – The New York Times, The Guardian, Der Spiegel, Le Monde, and El País. Additionally, it also became known for exposing a video (known as "Collateral Murder"), referring to the Iraq War, of a US military helicopter deliberately attacking Iraqi civilians and, among them, a Reuters photographer and his driver. (BENKLER, 2011; CURRAN, GIBSON, 2012). The actions of the WikiLeaks group led scholars to rethink the landscape of diplomacy and secrecy following the document revelations. (HOOD, 2011; PAGE, SPENCE, 2011; BENKLER, 2011). The former principal spokesperson of the organization, Julian Assange, currently resides in asylum at the Embassy of Ecuador in London, England. The WikiLeaks group's website on the Surface Web provides details about the Tor software and explains to interested users the necessary procedures to install the program on their network access device. (WIKILEAKS, 2016).

Chelsea Manning, previously known as Bradley Manning, served in the American army during the Iraq War as an Intelligence Analyst, being responsible for the leak of secret documents to the WikiLeaks organization over several months, serving as its principal source. (ROTHE, 2013; MERCK, 2015). Manning was subsequently arrested by American authorities – accused of violating the Espionage Act and other crimes against the USA – and sentenced to 35 years in prison on August 21, 2013. (HACKL; BECKER; TODD, 2016). She received a presidential pardon from the 44th American president, Barack Obama, and was released in May 2017. (PILKINGTON, 2017).

Edward Snowden, former employee of the company Booz Allen Hamilton, which maintained contractual services with the American government, was responsible for providing to the British newspaper The Guardian documents related to the PRISM program – whose objective was the collection of personal data of millions of individuals through mass digital espionage conducted over Internet communications. (LANDAU, 2013). The collection of documents leaked by Edward Snowden became known in the literature as "The Snowden Files." (CHADWICK; COLLISTER, 2014). The PRISM program was responsible for collecting metadata of domestic US communications, storing them in cloud service providers. (LANDAU, 2013). The British agency Government Communications Headquarters (GCHQ), equivalent to the NSA for the USA, permitted the surveillance of the American agency over British citizens. (CHADWICK; COLLISTER, 2014). After the revelations in 2013, Snowden received asylum from the Russian government and took up residence in the country. (MURATA; ADAMS; PALMA, 2017). Since then, he has advocated in favor of privacy and supported the Tor Project organization and the network maintained by it. (LEE, 2015). The anonymous network is, in fact, a target of attacks by the NSA and GCHQ – however, without success. (BALL; SCHNEIER; GREENWALD, 2013).

The newspapers The Guardian and The New Yorker both presented secure channels, via the Tor anonymous network, so that tips to journalistic editorial offices could be made by the public using the Internet. In 2013, the newspaper The New Yorker launched the anonymous information-sharing service **Strongbox**, which functions via Tor and allows shielded communication between journalists and sources. (PILKINGTON, 2013). Similarly, the newspaper The Guardian launched in 2014 the anonymous information-sharing platform **SecureDrop System**, so that whistleblowers could submit confidential documents to journalists of the institution. (BALL, 2014).

The **X-Net Group** is a cyberactivist group composed of more than 200 volunteers that operates in Spain along the lines of WikiLeaks but is involved in the country's politics and courts of justice. The group created a communication channel, via the Tor anonymous network, so that individuals could share confidential documents and assist in the fight against corruption. Only volunteers registered as "journalists" have access to the documents, for legal reasons. In October 2014, the group was responsible for denouncing corruption schemes involving high-ranking officials of the bank Bankia – a Spanish bank founded in 2010 during Spain's financial restructuring process. (ASSOCIATED PRESS, 2014).

Three years after Snowden's revelations, **Harold T. Martin III**, a former lieutenant of the American Navy, was arrested by US government authorities on charges of espionage and theft of confidential documents. Like Snowden, Harold Martin also worked for the company Booz Allen, which maintained contractual services with the NSA. The authorities discovered large quantities of secret government documents at his residence, whose content consisted of files from the period 1996–2016. The former agent, trained in computer security, pursuing a doctorate in "Information Security Management," Martin maintained communications in the Russian language and used cryptographic technologies that enabled online anonymity. In particular, the "Tails" operating system that redirects data traffic through the Tor anonymous network. (ASSOCIATED PRESS, 2016).

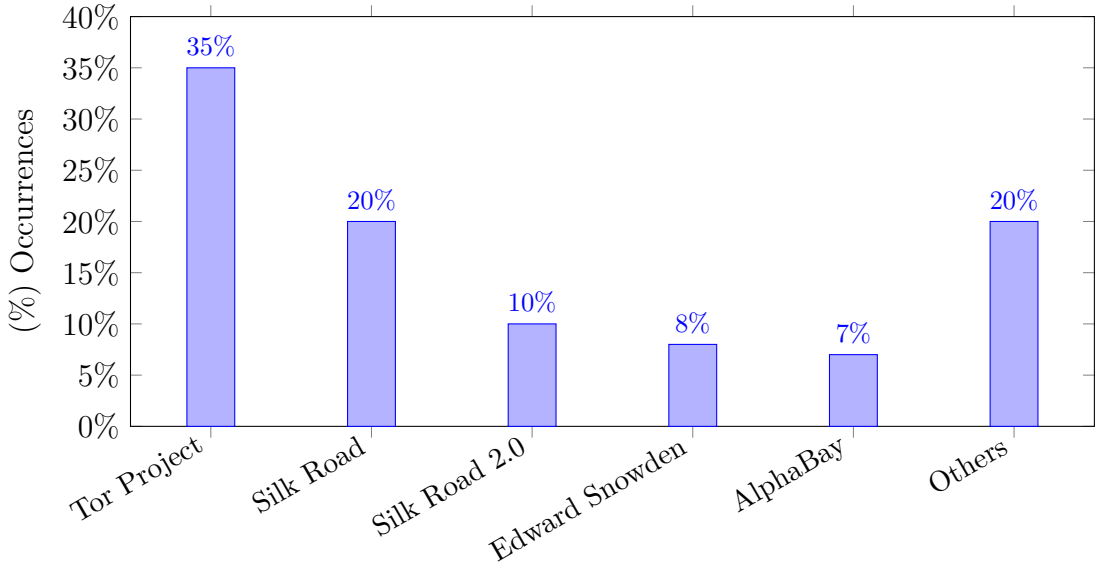
The non-profit organization **ProPublica** is considered the largest independent investigative newsroom in the world, headquartered in New York and a Pulitzer Prize winner. It was created by the charity foundation "The Sandler Family Supporting Foundation," which donates approximately 10 million dollars annually to the organization with the objective of strengthening democracy. (BROWNE, 2016). ProPublica's investigative journalism launched a news platform on the Dark Web in 2016, through the Tor anonymous network – whose objective is to protect the communications of users and the servers that store the information. Since 2016, users in countries that censor the web, such as China, can visit the ProPublica platform on the Tor network to follow news without fearing censorship and the tracking of data and activities. Furthermore, users can also share secret documents and information through ProPublica's whistleblowing service on the anonymous network. (JACKSON, 2016).

The "Privacy" category is composed of the actor Doxbin, one of the pages of the Tor anonymous network that seeks to disclose personal data and private information of individuals on the network.

The page on the Tor anonymous network, **Doxbin**, was shut down in 2014 by joint police authorities during Operation Onymous. (FOX-BREWSTER, 2014). The Doxbin page practiced what became known in the literature as "doxing" – the theft of personal data with the objective of maliciously denigrating or discrediting individuals. (LIBICKI, 2017). The practice of doxing is considered an abuse whose objective is to harm one of the parties through the disclosure of sensitive data and information, and its motivations are varied: from personal to political reasons. (SNYDER et al, 2017). According to Fox-Brewster (2014), as soon as the page was taken down, the individual with access to the servers, known by the online alias "nachash," leaked the site's records in the hope that others could identify the means by which police authorities captured the domain. However, despite having confiscated the domain, the content of the servers remains within reach of the Doxbin site's collaborators – requiring "only" that they configure a domain for public access. (FOX-BREWSTER, 2014).

Of the total of 25 actors present in the database of this research, 5 account for 80% of the total number of occurrences. The Tor Project accounts for approximately 35% of total occurrences, followed by the online marketplace Silk Road and its later version, Silk Road 2.0. The former NSA agent, Edward Snowden, accounts for approximately 8% of occurrences, while the online marketplace AlphaBay accounts for approximately 7% of the total.

Chart 3 – Top 5 Actors by Percentage of Occurrences (2007–2017)



Source: Author.

4.2 Diffusion of Power: Actors, Thematic Groups, and Total Occurrences

Our analysis of the diffusion of power was conducted based on the three defined dimensions – authority, control, and outcomes. Each dimension had its own analysis, since the dimensions are distinct and the variables (of the same name) operate on different scales.

The analysis was carried out in three segments: first, at the level of actors – in which each actor was analyzed individually based on the occurrences in which they are the protagonist; second, at the level of thematic groups – at which point the set of actors with similar themes was gathered and the total occurrences of the group were analyzed; and third, in a general manner – the analyses were conducted based on all occurrences from the period between 2007–2017. With this, we sought to provide a diagnosis of the diffusion of power according to journalistic publications from the aforementioned period regarding the low-latency anonymous network Tor – in order to answer our research question. We emphasize that the individual analysis by actor provides sufficient input to identify the preponderant actor within each thematic group. The general table containing the analyses of each dimension by actor, thematic group, and total occurrences can be found in the appendix of this dissertation.[161]

4.2.1 The "Authority" Dimension

The thematic group with the highest number of occurrences is Online Marketplace (57 occurrences or 40.7% of the total). In the **authority** dimension, we verified that there was a decrease in the authority of the actors that compose the group in 47 occurrences. In the remaining 10 occurrences there was a tie: in 5 occurrences the authority remained stable, and in another 5 there was growth in authority. In total, we perceive that there was more decrease in the authority of the actors that compose the "Online Marketplace" group than stability or growth. It is worth remembering that the actors that compose this group are the anonymous "black markets" of the low-latency Tor network – responsible for administering a meeting space between sellers and buyers of illicit products, acting as promoters of commercial transactions of drugs and narcotics, primarily.

There are two hypotheses that explain the decrease in authority of these actors that operate via the anonymous network. The first hypothesis is that the newspapers selected for this research prioritize the publication of news that reports the arrest of the administrators responsible for the black markets, or the closure of the online marketplace domain on the anonymous network – that is, public access to the marketplaces through Tor. The second hypothesis is that, in fact, more closures and arrests are occurring than proliferation of anonymous markets and success cases – that is, those that operate freely

[161] See "Appendix 9 – Analysis of Diffusion of Power by Actor and Group."

via Tor, without interference from police authorities.

Be that as it may, the decline in authority of the anonymous markets reflects the "distrust" of peers and stakeholders (market customers, private citizens interested in consuming the products sold, and individuals interested in administering similar markets and earning proceeds from sales commissions) regarding the markets in question. If the published news reflects arrests and closures of anonymous markets, the authority of these does not remain stable or growing over time – on the contrary, it demonstrates decline. This decline is a reflection of the power relationship between the authority of the State and the authority of anonymous markets: while the latter see their authority decline (due to market closures and administrator arrests), the former observe their authority grow before society as they achieve the results they themselves aimed for. Therefore, based on the analyzed occurrences, derived from news articles published by the ten largest newspapers by number of users per click, we can affirm that the power of online markets that operated on the Tor anonymous network between 2007 and 2017, in the authority dimension (which concerns the trust of peers and stakeholders), suffered more decline than stability or growth.

The second thematic group with the highest number of occurrences, 54, is the "Surveillance Circumvention" group. We verified that the largest share of these occurrences reflects growth or stability of the authority of the actors that compose the group. In 27 occurrences there was growth in authority; in 18 occurrences it was verified that authority remained stable; only in 9 occurrences was there a decline in authority. The stability and growth of the group's authority reflects the success of non-state actors both in circumventing, through the Tor anonymous network, the censorship regime in the digital domain imposed by authoritarian countries such as China and Iran, and in maintaining the anonymity of their identities and operations. In particular, the highlight goes to the actor Tor Project which, through the maintenance and improvement of the network, as well as the adoption of techniques pertinent to activism in general, was largely responsible for offering an alternative communication channel for Internet navigation. The increase in authority of non-state actors, or at least the stability of this authority, seems to reflect the difficulty of States in general in maintaining the regime of censorship and blocking of cyber regions for public access. Therefore, based on the analyzed occurrences, we can affirm that the power, in the authority dimension (which reflects the trust and interest of peers), of actors that offer an alternative communication channel to censorship and blocking imposed by rigid state mechanisms, increased during the period between 2007 and 2017.

The third thematic group by order of occurrences is "Journalism & Whistleblowing," with 21 occurrences examined. As with the previous thematic group, we verified that the actors in this group have experienced growth in authority, or at least stability. In 16 occurrences, growth in authority was verified, and in 5 occurrences, stability. In

no occurrence was a decline in the authority of any actor in the group found, whether whistleblower, journalist, or activist group working with sensitive information. Within the group, the highlight was Edward Snowden, with 11 occurrences, of which 9 reflected growth in authority and 2 reflected stability. Snowden's revelations detailed, through files and documents originating from the NSA, the mass digital surveillance perpetrated by the US government and its allies. From the reading of the articles, an increase in trust placed in the figure of the whistleblower by peers and stakeholders was verified – including because he had formally been an operative part of the surveillance scheme.

In this sense, from the analysis of occurrences made regarding the "Journalism & Whistleblowing" group, we can affirm that there was an increase in the power of these non-state actors in the authority dimension. One hypothesis for the absence of decrease in authority of these actors is that the Tor anonymous network, during the analyzed period, provided a secure means of communication so that whistleblowers of great relevance could transmit to journalists and other professionals who deal with confidential information documents and files that substantiate the disclosures. That is, the low-latency anonymous network Tor offered a communication channel seen as sufficiently secure to attract high-risk whistleblowers – whether due to their position within the governmental apparatus, or due to the confidential nature of the information in their possession. Furthermore, it also served as a means of receiving confidential information by the editorial body of conventional newspapers and activist organizations.[162] For this reason, whistleblowers, newspapers, and activist organizations saw the trust placed in them by peers and stakeholders increase during the investigated period.

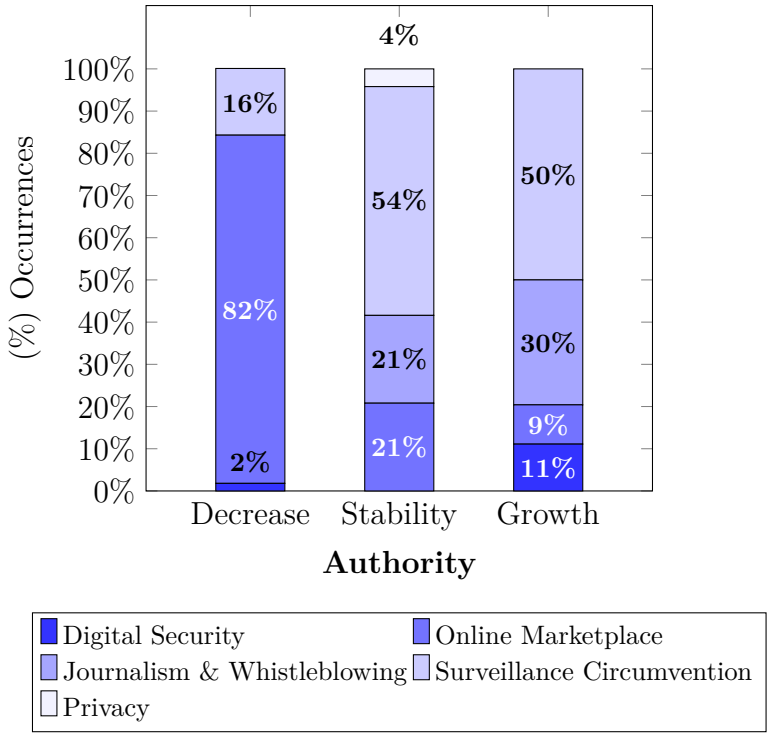
The fourth thematic group, "Digital Security," accounts for 7 analyzed occurrences. Each actor in the group was responsible for 1 occurrence, totaling 7 actors and 7 occurrences. With the exception of the actor Freedom Hosting, growth in authority was verified in the remaining actors. Upon suffering infiltration by malware, which is believed to have been implanted by FBI agents, the Freedom Hosting server, accessible only through the Tor anonymous network, allowed authorities access to the information stored on it. It is worth remembering that the server hosted files and documents largely pertaining to child pornography. For this reason, the authority of the Freedom Hosting server suffered a decline, given that the trust of peers and stakeholders in allocating and accessing information on it entered decline due to the fear of discovery of the identities behind the visiting users. The remaining actors comprise malicious software, researchers, and digital security professionals who operate on the anonymous network – these saw the

[162]In addition to Edward Snowden, other whistleblowers who appeared in the analyzed occurrences were Chelsea Manning, responsible for transferring secret documents from the American armed forces to the WikiLeaks organization, and Harold T. Martin, who like Edward Snowden, also worked for the company Booz Allen Hamilton that provided services for the NSA. As for the WikiLeaks organization, the activist group X-Net Group, the newspaper The Guardian (SecureDrop System), The New Yorker (Strongbox), and ProPublica offer communication and document submission channels, through the Tor anonymous network, so that whistleblowers can carry out their disclosures.

trust placed in them by peers and stakeholders increase.

The fifth and last group, "Privacy," comprises a single observation of a single actor, the Doxbin page responsible for gathering in a single location the exposure of private data of individuals. It was verified that there was no growth or decrease in the authority of this page, but rather stability of authority. That is, the trust of peers and stakeholders did not increase, nor did it decrease; it merely maintained itself.

Chart 4 – (%) Occurrences by Thematic Group in the Authority Dimension (2007–2017)



Source: Author.

Through the percentage chart of diffusion of power in the authority dimension, it is possible to make some comparative interpretations between the thematic groups.

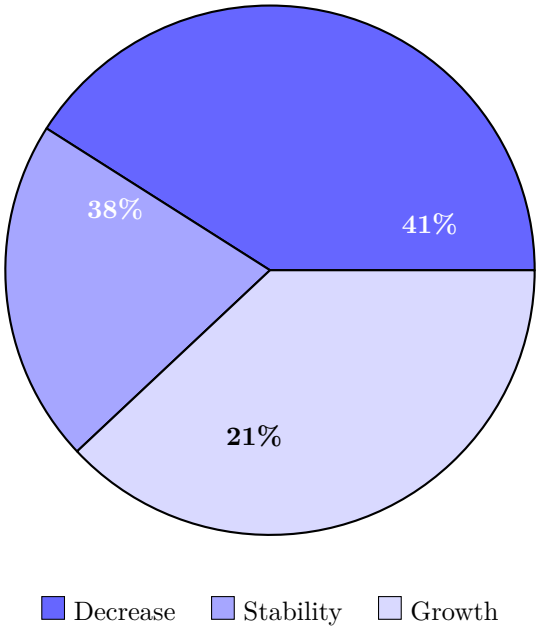
Among all thematic groups, the one with the highest percentage of decrease in authority is the "Online Marketplace" group. In fact, from the journalistic articles analyzed in this research, it was verified that the majority exposed two major subjects – those related to the arrest and trial of the administrators behind the anonymous markets, and those related to the closure of the domain by police authorities. Both subjects affect the degree of trust placed in the markets that operate on the Tor anonymous network and diminish the authority of these before peers and stakeholders.

The "Surveillance Circumvention" group is the one with the highest percentage of stability and growth in authority. The analyzed newspaper articles evidenced, primarily, two consequences of the operations of the actor Tor Project, responsible for the maintenance and improvement of the anonymous network. The first consequence refers to the

censorship and blocking of content in the cyber domain by authoritarian States. The Tor Project offers alternative access to prohibited content, becoming an important ally of activists and whistleblowers in regions whose information governments seek to control. The second refers to the protection of the content of messages exchanged through the anonymous network and the protection of the identity of users who operate on the network. These protections circumvent the surveillance system perpetrated primarily by governmental actors. For these reasons, the trust placed, by peers and stakeholders, in the activist organization Tor Project has grown – which is reflected in the analysis.

It is also worth highlighting the "Journalism & Whistleblowing" thematic group, which stands as the second group with the highest percentage growth in authority – behind only the "Surveillance Circumvention" group. The growth in authority reflects the increase in trust placed by peers and stakeholders in the group's actors for using the anonymous network as a channel for transmitting sensitive information – given that the network offers protection of privacy and anonymity to users.

Chart 5 – Diffusion of Power, Dimension "Authority" (%) Occurrences (2007–2017)



Source: Author.

The chart above pertains to all occurrences between 2007–2017 that were analyzed by this research, without identifying actors or thematic groups.

It is possible to observe that in the "authority" dimension, the highest percentage of occurrences analyzed in this research refers to the decrease in authority of non-state actors. The second highest percentage of occurrences indicates that there was growth in the authority of non-state actors, while 21% of occurrences points to the stability of

authority. However, if we admit that the diffusion of power occurs from the non-decrease of non-state authorities, then we can consider that the diffusion of power, in this case, is the result of the percentage of growth and, at most, of stability of authority. That is, at a minimum, the non-state actor that already possessed some degree of authority managed to maintain this degree, while the one that had no degree of authority saw its authority grow – or rather, go from *no* authority to *some* authority. This scenario is different from the one that only considers the growth of authority, for in that case, all other non-state actors that *already possessed* some degree of authority are excluded from the analysis. For this reason, we can think that the diffusion of power is occurring from the moment that, at a minimum, a non-state actor with some degree of authority over matters derived from the set of values originating from social organization is verified.

Thus, in the set of occurrences analyzed by this research, we observe that in approximately 59% of them, the authority of the non-state actor, belonging to the knowledge structure, grew or at least did not diminish by reason of using the low-latency anonymous network Tor.

4.2.2 The "Control" Dimension

In the **control** dimension, it is noted that all actors in the "Online Marketplace" category held some degree of control over relevant objects – in this case, the online marketplace itself and payment mechanisms. In 29 occurrences, partial control of the anonymous market over the virtual meeting space between buyers and sellers and the payment system used by them to carry out commercial transactions was observed. In 28 occurrences, absolute control of the anonymous markets was observed. There were no cases in which control was considered "none."

In the news articles published on the topic, in a significant portion, the absolute control of the online market is verified. In these occurrences, the control of the market is absolute because it is responsible for providing the virtual meeting space between buyers and sellers and also the payment system in its entirety – not relying on third parties, such as banks or card networks, etc. The payment system, in this case, is based on cryptographic virtual currency (generally Bitcoins) and depends on the approval of the person(s) in charge for the financial transaction between seller and buyer to be executed.[163] The possession of control over the virtual market environment allows it to have the power to permit or deny access of interested parties to commercial transactions. If the person responsible for the marketplace has control of both – the virtual meeting space between buyers and sellers and the payment system – it is said that they have absolute control over the operation

[163]A mechanism known as "escrow," detailed earlier. The administrator of the online marketplace, after confirmation from both the seller and buyer regarding the payment and receipt of the purchased merchandise, authorizes the definitive transaction of payment in cryptographic currency, collecting a portion of the amount for themselves (commission).

of the anonymous market. If the person responsible for the marketplace has only control of the virtual space, and not of the payment system, we state that the control over the object is partial – since a part of the control of the anonymous market's operations is at the disposal of another entity or institution.[164]

As with the previous group, in the "Surveillance Circumvention" group, all actors held some degree of **control** over objects relevant to the execution of their activities. The highlight is the absolute control of the functioning of the Tor anonymous network by the actor Tor Project – responsible for its administration, maintenance, and improvement. From the analysis of occurrences, it was verified that the Tor Project has absolute control over the removal of any suspect node from the anonymous network – which occurred on some occasions. Furthermore, the Tor Project also has control over the creation of "bridges" that allow access to the network by users who find themselves, in some way, blocked from accessing the network through standard means.

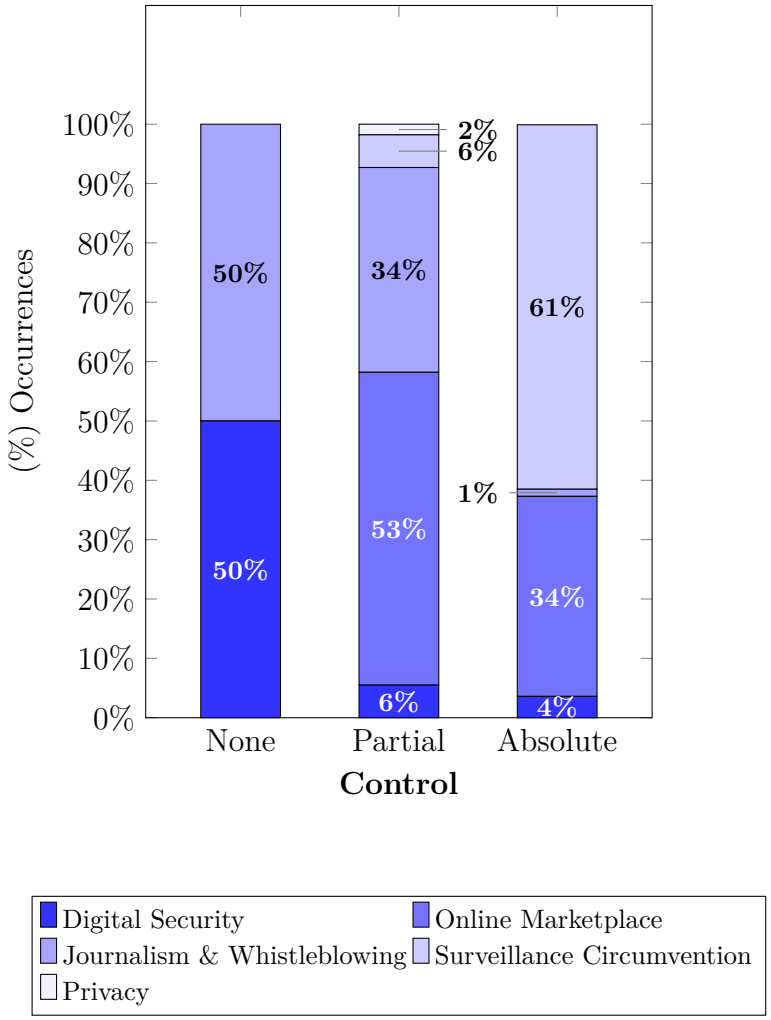
Observing the diffusion data of the "Journalism & Whistleblowing" group, it is possible to perceive that the majority of actors who compose it held some degree of control over objects considered relevant for achieving desired outcomes. This control was, predominantly, partial – with 19 of the occurrences (out of a total of 21 occurrences).

In the "Digital Security" group, it was verified that the majority of actors who compose the group have some degree of **control** over objects pertinent to the achievement of their objectives operated through the Tor anonymous network. These objects range from servers located on the network to the anonymous network itself. Of the total of 7 occurrences, the actors have partial control over objects in 3 occurrences; and absolute control in another 3 occurrences. The only actor without any control over an object relevant to the operation of their activities is the security specialist Dan Egerstad, who observed security breaches of embassies on the anonymous network.

Regarding the "Privacy" group, from the analyzed occurrence, it was possible to identify that the actor held partial **control** over the servers that contain the collection of personal information of numerous individuals.

[164]The interpretation of absolute or partial control of the anonymous marketplace derives from the analyzed occurrences: if it is explicit that the anonymous marketplace operates with its own payment system, we say that the control is absolute. If it is not explicit, we say that the control of the anonymous marketplace is partial.

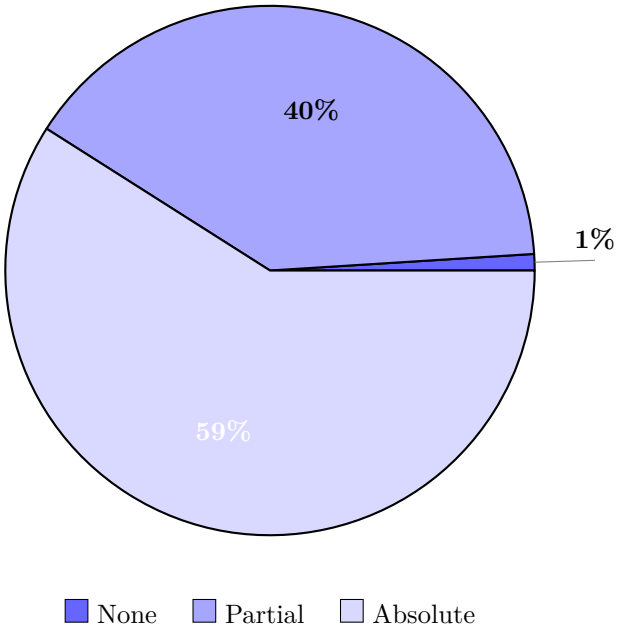
Chart 6 – (%) Occurrences by Thematic Group in the Control Dimension (2007–2017)



Source: Author.

If we observe statistical data comparing percentages of thematic groups among themselves, in the control dimension, we observe that the thematic groups "Journalism & Whistleblowing" and "Digital Security" were those that least presented control over some relevant object to their operations in percentage terms. Both groups had a single occurrence for "no" control. The "Online Marketplace" group was the one that most obtained partial control over objects (in this case, the virtual meeting environments between buyers and sellers and the payment system through which financial transactions were carried out), followed by the "Journalism & Whistleblowing" group, whose actors partially controlled information, documents, and confidential files (in the case of whistleblowers) and secure channels for the transmission and publication of this information (in the case of journalists and activists). The highest percentage of absolute control was relative to the "Surveillance Circumvention" thematic group, whose actor Tor Project is responsible for the maintenance and administration of the anonymous network.

Chart 7 – Diffusion of Power, Dimension "Control"
(%) Occurrences (2007–2017)



Source: Author.

In the "control" dimension, we observe from the chart that in 59% of occurrences analyzed in this research, the non-state actor originating from the knowledge structure held absolute control of an object while exercising activities in the cyber domain. In 39% of occurrences, this control was partial; while in only 2% of occurrences the control was none. In other words, in 98% of occurrences the non-state actor held some degree of control over objects originating from the knowledge structure during their operations on the Tor anonymous network.

4.2.3 The "Outcomes" Dimension

In the **outcomes** dimension, in the majority of occurrences (42 occurrences) of actors in the "Online Marketplace" group, it was possible to observe alteration of the status quo with effects on reality. In only 15 occurrences was non-alteration of the status quo verified – that is, its maintenance. In other words, the analyzed occurrences provided sufficient input to affirm that, by reason of using the low-latency anonymous network Tor, the online marketplaces that operate on this network managed to effectively commercialize illicit substances, such as drugs and narcotics in general, in the real world.

In the "Surveillance Circumvention" group, it is observed that, in the **outcomes** dimension, there was no alteration of the status quo in the real world in the majority of occurrences. The status quo in question reflects two situations: first, the maintenance of the blocking and censorship of certain content on the Internet by authoritarian countries;

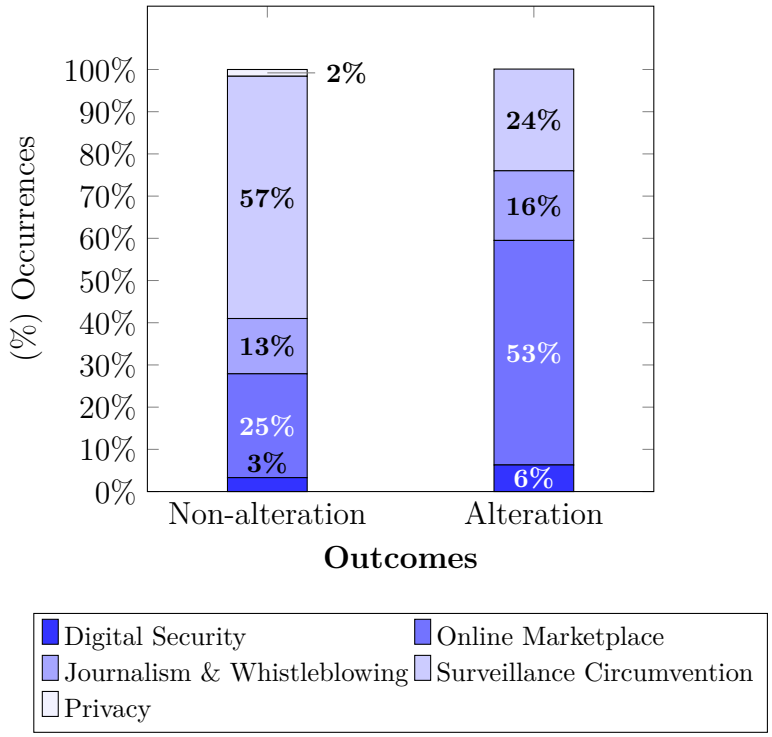
second, the maintenance of the anonymity of operations and identities of users who use the Tor anonymous network. The first situation reflects a reduced number of occurrences, while the second situation reflects the majority of analyzed occurrences. In approximately 65% of occurrences there was no alteration of the status quo mentioned above; while in approximately 35% of occurrences, there was alteration of these status quo conditions.

Regarding the "Journalism & Whistleblowing" group, it is possible to affirm that there was alteration of the status quo, with consequences for the real world, in the majority of occurrences: 13 alterations of the status quo compared to 8 occurrences of non-alteration.

In the "Digital Security" group, in 70% of occurrences of this thematic group there was alteration of the status quo in the real geographical world. In 30% of occurrences the status quo remained unaltered.

Regarding the "Privacy" group, no alteration of the status quo in the real world was observed from the occurrences – evidence that, despite gathering personal data and information of individuals, this information was not used in the real world for any purpose.

Chart 8 – (%) Occurrences by Thematic Group in the Outcomes Dimension (2007–2017)

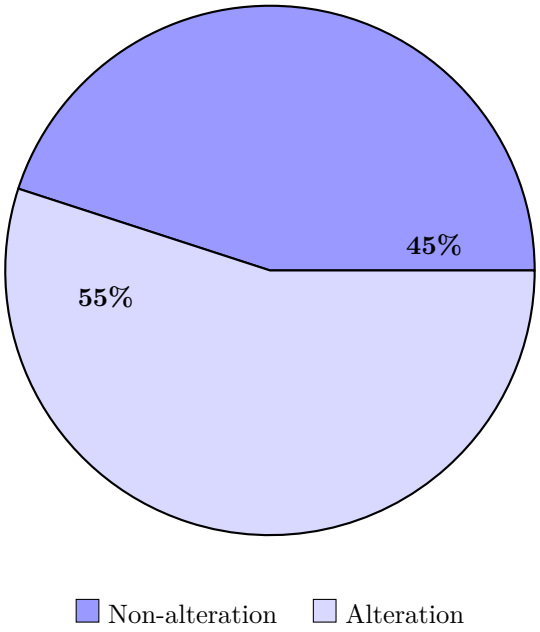


Source: Author.

In the outcomes dimension, we verify through the percentage chart of occurrences that the theme that most achieved alteration of the status quo, with consequences for the real geographical world, was the "Online Marketplace" group. The arrest and trial of administrators of anonymous online markets evidence the commercial transaction of illicit substances, drugs, and narcotics through the low-latency Tor network. In general,

as noted by Sedghi (2014), there was an increase in the consumption of these substances due to relatively secure access to the anonymous network's markets. The thematic group that least achieved alteration of the status quo in the real world was "Surveillance Circumvention." The hypothesis is that shielding against surveillance perpetrated in the cyber domain is a passive act – that is, it will only affect the status quo if the entity responsible for surveillance succeeds and acts upon the individual under surveillance – and not the contrary.

Chart 9 – Diffusion of Power, Dimension "Outcomes"
(%) Occurrences (2007–2017)



Source: Author.

Regarding the last dimension, "outcomes," it was possible to verify that in 56% of occurrences analyzed by this research there was alteration of the status quo with consequences for the real geographical world. That is, in more than half of the occurrences, non-state actors achieved success in altering the status quo by reason of using the low-latency anonymous network.[165]

[165]With the exception of the actor Tor Project, we can say that the actors who achieve success in altering the status quo act in the direction of achieving desired outcomes. The Tor Project, on the other hand, acts with the purpose of non-alteration of the status quo in the real world, since this organization (responsible for performing maintenance and improvements on the network) seeks the protection of users' privacy and the anonymity of exchanged messages. The alteration of the status quo indicates, at times, that the anonymity of users and messages did not have effectiveness.

4.3 Analysis of the Diffusion of Power in the Context of the Tor Anonymous Network

We believe that sufficient evidence exists to believe that the diffusion of power operates in three distinct dimensions. We can affirm that the diffusion of power is underway when there is growth of non-state authorities (or at least the maintenance of already existing non-state authorities); when non-state actors are capable of controlling objects relevant for achieving desired ends; and when these, through their actions, succeed in altering the status quo – whose consequences affect the real geographical world (since in this research we addressed the activities and operations of subjects in the cyber domain). The three dimensions denote power as they corroborate the analytical framework proposed by Strange (1988) that culminated in the field of IPE. Although she herself did not address the three dimensions, when we analyze the phenomenon of diffusion of power through these dimensions, we are able to ascertain its existence or absence.

This affirmation derives from the following logic: when there is concentration of power in the figure of the State – that is, the opposite of the diffusion of power defined by Strange (1996) – this means, for the three dimensions, that (1) the State has the leadership of authority in matters derived from the values originating from social organization – which includes the knowledge structure; (2) the State is the one that most holds control over objects pertinent to achieving results desired by it; (3) the power of the State is such that it succeeds in altering the status quo – that is, it is capable of achieving the objectives it aims for. The diffusion of power reflects in these three dimensions the contrary logic: the State does not hold leadership in the primary structures (and, in this case, in the knowledge structure); it is not the only one with the capacity to control objects relevant for the achievement of proposed objectives; and it is not the only one capable of making alterations to the status quo. However, it should be noted that this dissertation is exploratory in character – that is, it does not intend to offer fixed answers on a challenging topic, although it reflects on specific points of the literature.

In sum, we observe the diffusion of power occurring in the three dimensions for the majority of non-state actors positioned in the knowledge structure who carried out their operations via the low-latency anonymous network Tor.

4.4 Conclusion

This chapter sought to carry out an analysis of the diffusion of power in three dimensions. This analysis focused on a database assembled from journalistic articles originating from the ten largest newspapers in the world by number of users per click. This database brought non-state actors, positioned within the knowledge structure, as protagonists of

actions perpetrated via the low-latency anonymous network "The Onion Router." This network became known for offering an alternative communication channel in the cyber domain – beyond the reach of governmental authorities – that aims to ensure the privacy of users and the anonymity of messages exchanged through it. The technology developed by the organization responsible for the Tor network is derived from knowledge and information about cryptographic and routing techniques, among others, that accumulated primarily during the 1990s. This network became especially known to the general public after 2013 and 2014, when media outlets published news related to the anonymous markets that operate on it, as well as arrests and trials of those responsible, in addition to being commonly associated with whistleblowers and journalists due to the protection it provides to communications.

From the conceptual foundation regarding the Tor anonymous network as an important part of the knowledge structure in the 21st century, explored in chapter two, we sought to present the method by which we elaborated the database used in this research. This database was the result of investigations of news articles published by 22 newspapers in total, originating from four countries: the United States, England, India, and China. Through each newspaper article, we sought to identify non-state actors positioned in the knowledge structure, as well as their actions carried out via the Tor anonymous network. The composition of this research's database resulted in 139 rows and 14 columns, and allowed us to identify 25 actors, which we grouped into 5 thematic groups – since it was possible to identify similar themes in the journalistic articles. From the available information, we were able to carry out the analyses of diffusion of power in three dimensions and according to the theoretical framework presented in the first chapter of this dissertation.

Our analysis of diffusion of power, in addition to encompassing the three dimensions, aimed at presenting three segments, as a means of providing a systematic view of the database. These three segments were about: the actors, the thematic groups, and the total occurrences between the years 2007 and 2017. In general, we were able to observe that, in the authority dimension, the Tor anonymous network contributed to the increase – or at least stability – of the authority of actors in the majority of occurrences. In the control dimension, we identified that nearly all non-state actors possessed control over objects in the cyber domain. These objects were pertinent to achieving the results desired by them. In other words, we verified that the majority of non-state actors held some degree of control over objects in the course of their operations. And these objects, which operate in the cyber domain, are abstract constructions born of accumulated knowledge originating, in our analysis, from civil society. The command of these objects by non-state actors in our analysis demonstrates the relevance of knowledge and information in cyberspace – which leads us to suppose that the cyber dimension is an important domain for the knowledge structure in the 21st century. In the outcomes dimension, it was possible to observe that in more than half of the occurrences, non-state actors

succeeded in altering the status quo with consequences for geographical reality (that is, non-cybernetic).[166] This success in altering outcomes occurred by reason of using the Tor anonymous network which, through its technology and nature, allows the dynamic through which the actors operated in order to achieve these results.

In sum, the Tor anonymous network contributes to the diffusion of power in the three dimensions based on its technological specificities that differ from other communication channels. In our analysis, this diffusion of power was evidenced in the majority of occurrences in the database used by us for the purposes of this research. It should be noted that this database is the result of journalistic approaches that aim to notify the public about questions of relevant general interest. It was through the Tor network that various actors were able to carry out their operations in order to affect the status quo. Thus, the difference between the Dark Web and the Surface Web is highlighted for purposes of outcomes and for the diffusion of power. There are reasons to believe that the actors analyzed in this research would not have achieved the same results had they operated through other communication channels with technology and nature different from the anonymous network – such as, for example, the Surface Web.

[166] With the exception of the actor Tor Project.

Final Considerations

The discipline of International Political Economy gained relevance in International Relations studies by, paradoxically, offering an approach to the International System that includes non-state actors. The British scholar Susan Strange inaugurated a vision of actors, activities, and individuals in the International System from a perspective that seeks to answer political-economic questions through four primary structures. This new approach includes non-state actors and brings academic studies closer to practical reality, since, although States are those ultimately responsible for sustaining order and security within national territories, they cannot be considered the only authorities that affect people and services.

Although not a theorist, Strange (1988) was a scholar and erudite who provided a vision of the operations of the international political-economic fabric in a way that encompasses four structures that, according to her, lie at the core of any society, whether at the global or local level: security, production, finance, and knowledge. After all, all minimally organized societies concern themselves with security and survival; with the production of food, tools, and products in general; with the creation of credit; and with the accumulation of knowledge and information that can be passed on between generations. The international system is observed, therefore, from an analytical framework that allows the participation of actors beyond the State – since these are not the only ones that affect the four structures and people. Strange's IPE paradigm aims to understand the way in which power operates in the socio-political-economic fabric and, for this reason, she directed criticism at both economists (for ignoring the element of power in their analyses) and political scientists (for ignoring important aspects of the economy). This new paradigm seeks to provide sufficient resources for analyses that cover both segments within a global, or rather, international context.

It is from the IPE paradigm addressed in the 1988 work that Strange gathers the foundations that underpin her vision of the diffusion of power, affirming that State power has declined, in a qualitative sense, due to the rise of other authorities acting globally. According to her, such authorities have sufficient power not only to allocate basic values of human organization in society, but also sufficient capacity to alter outcomes and redefine options for others. These diverse non-state authorities are broadly embedded within the four primary structures. Their indirect power, or rather, structural power, is precisely

the result of the action of structural dynamics, while direct power is well known in the discipline of International Relations: also known as relational power.

In this research, we sought to analyze the diffusion of power through the low-latency anonymous network "The Onion Router." This network operates through the Internet, being part of the set of networks that form the "Dark Web" – a region of the web where there is an active effort to maintain the anonymity of communications and users. This anonymous network seeks to be a relevant communication channel in the face of digital surveillance perpetrated by governmental and private entities. As a means of communication, it is situated within the knowledge structure, one of the primary structures initially defined by Strange in 1988. According to her, in addition to encompassing beliefs, principles, and moral conclusions, this structure also encompasses what is known and understood, and extends over the communication channels through which information is communicated. For this reason, we can affirm that the low-latency anonymous network Tor is part of the knowledge structure. And, as belonging to the knowledge structure, one verifies the existence of subjects, also positioned within this structure, who operate on the anonymous network. If Strange (1988) indicates that the structural analytical framework can be understood from both a global and local perspective, there is no reason to suppose that it would be unfeasible to use this framework for observations in the cyber domain. After all, different state and non-state actors operate in the cyber environment, affecting people and services offered in this domain, even though she herself did not address this domain specifically.

This dissertation sought to answer the research question in order to verify in what way, and to what extent, the anonymous network The Onion Router contributes to the diffusion of power in the knowledge structure. As seen, both the knowledge structure and the phenomenon of the diffusion of power were elements defined by Strange (1988, 1996) and, for this reason, our research was based on her works during the investigation of the phenomenon in this specific communication channel of the cyber domain. After considerable examination of the works, we identified two relevant points that bear on our analysis: first, the finding that the diffusion of power operates in three dimensions; second, even though she did not address the cyber domain, Strange indicated the importance of the technological revolutions that were occurring at the end of the 1980s and 1990s.

The first dimension is that of "authority." In this dimension, we sought to demonstrate that Strange's considerations regarding power are treated, at times, as considerations regarding authority. However, although the differences between "power" and "authority" are subtle, we believe there are sufficient indicators in the author's works to affirm that these two elements are not synonymous. Authority can be viewed in two ways: as an entity that gathers the trust of peers and stakeholders upon itself; and also as the very exercise of power. In the first instance, we refer to "being an authority" – which can be achieved through transfer, grant, concession, delegation, etc. This authority, therefore,

can arise formally or informally. In the second instance, we refer to "exercising authority." This exercise of authority implies the use of power, since exercising authority means that the authority uses all means available to it to put desired ends into practice. In other words, authority exercises power in order to realize its will. We emphasize, however, that both forms of authority can only be tested, verified, and examined through the third dimension – outcomes.

The second dimension refers to "control." Initially, we verified that on different occasions in the analyzed works, Strange (1988) indicates the control of an object by an actor to denote that actor's power. We gathered the citations in which the author makes these assertions and identified both the actor in question and the object controlled by them, giving rise to "Appendix 3" of this dissertation. This gave us sufficient input to examine the role of control in conferring authority and power upon actors within a structure. In the case of the knowledge structure, the role of control proved to be essential since it lies at the core of the definition of power in the knowledge structure: power is attributed to those who occupy a prominent position, or a decision-making position, in the knowledge structure and falls upon (1) those recognized by society as holders of knowledge; (2) those responsible for its storage; (3) and those who control the channels through which information and knowledge are transmitted. For the purposes of analysis, in this dimension, we assumed that control can be none, partial, or absolute.

The third dimension refers to "outcomes." In this dimension, outcomes reflect the alteration of the status quo or its maintenance. The outcome attests to, or refutes, the authority of an actor and/or their control over an object they consider pertinent to achieving the desired result. That is, we can assume that an actor has authority – after all, "being an authority" demonstrates the trust of peers and stakeholders. This authority is not synonymous with power. However, at some point, the actor may exercise the authority invested in them (formally or informally) and alter the status quo in favor of a scenario desired by them. In this situation, one verifies that the authority, in fact, has power. But if the actor, upon exercising authority (or rather, power), does not bring about the alteration of the status quo in favor of a scenario desired by them, we cannot admit that the actor still holds authority. Authority, in fact, can only be determined on the basis of this dimension, of outcomes. Similarly, the relevance of an object for a given actor in the pursuit of a specific result can only be determined if control of that object is pertinent to the alteration of the status quo. If it is not, the actor's control of that object does not result in power.

Our investigation was limited to examining the diffusion of power in the domain of the anonymous network "The Onion Router." This investigation took place through the elaboration of a database containing occurrences derived from journalistic articles. These articles originated from the ten largest newspapers by number of visitors per click, as presented by Comscore (2012). The means by which the articles were selected to

compose the database was presented in the third chapter of this dissertation. From this composition, we were able to make some interpretations regarding, for example, the popularity of the Tor network from 2013 onward. Furthermore, we carried out analyses of the diffusion of power in three dimensions according to three distinct segments: first, we presented a table with the exposition of the 25 actors (originating from the journalistic articles); second, the actors whose news content was similar were grouped into the same "thematic group" and we made considerations about the diffusion for the groups; and third, we examined the diffusion of power through the total occurrences between the years 2007–2017. Through our analysis, we were able to verify that the diffusion of power occurs for the majority of verified occurrences. There are sufficient indications to interpret that the specific technological nature of the Tor anonymous network is a preponderant factor for the presence of the phenomenon in the knowledge structure in the 21st century.

Lastly, we also brought important considerations regarding the phenomenon of the diffusion of power under Nye's paradigm in relation to "cyberpower" that originates from cyberspace. Nye's discourse on power resembles Strange's discourse in that it concerns a "vertical" phenomenon, in which it is supposed that power is "diluting" in the global political and economic fabric from the State toward non-state actors. Nye also specifically affirms the existence of a cyber power (cyberpower), becoming the first major theorist in the field of International Relations to make considerations about power in the new domain of the 21st century. It is possible to perceive that the definition of cyber power, coined by Nye (2011), is intimately related to a set of resources that derive from the knowledge structure – albeit indirectly.

Finally, we presented charts, tables, and figures whose purpose was to serve as support for our analyses and to present the "findings" made during this present research.

Bibliographic References

ABERYSTWYTH UNIVERSITY (United Kingdom). International Politics Centenary. 2017. Available at: https://www.aber.ac.uk/en/interpol/centenary/. Accessed: 8 Aug. 2017.

AKHOONDI, Masoud; YU, Curtis; MADHYASTHA, Harsha V. LASTor: A Low-Latency AS-Aware Tor Client. IEEE Symposium on Security and Privacy. [s.l.], p. 476–490. Jul. 2012.

ALSABAH, Mashael; BAUER, Kevin; GOLDBERG, Ian. Enhancing Tor's Performance Using Real-Time Traffic Classification. In: ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 12., 2012, Raleigh. Proceedings. [s.l.]: ACM, 2012. p. 73–84.

ANDERSON, Daniel. Splinternet Behind the Great Firewall of China: Once China opened its door to the world, it could not close it again. Queue: Web Security, [s.l.], v. 10, n. 11, p. 1–10, Nov. 2012.

ANDERSON, Kevin. Using proxies to get around censors. The Guardian. London, p. 1–3. 01 Jul. 2009.

ARTHUR, Charles. The ransomware attack is all about the insufficient funding of the NHS. The Guardian. London, p. 1–2. 13 May 2017.

ASPRAY, William; CERUZZI, Paul E. (Ed.). The Internet and American Business. Cambridge: The MIT Press, 2008. 596 p.

ASSOCIATED PRESS (United States). Coldwater man among 15 arrests in international online drug probe. Michigan News. Michigan, p. 1–2. 16 Apr. 2012.

ASSOCIATED PRESS (United Kingdom). 'Dark Web' drug site challenge law enforcement. Daily Mail. London, p. 1–3. 07 Nov. 2014.

BACHRACH, Peter; BARATZ, Morton S. Two Faces of Power. American Political Science Review, [s.l.], v. 56, n. 4, p. 947–952, Dec. 1962.

BALDWIN, David A. Security Studies and the end of the Cold War. World Politics, [s.l.], v. 48, n. 01, p. 117–141, Oct. 1995.

BALDWIN, David A. Power and International Relations. In: CARLSNAES, Walter; RISSE, Thomas; SIMMONS, Beth A. (Ed.). Handbook of International Relations. London: Sage Publications Ltd, 2013. Ch. 11. p. 273–297.

BANKS, Michael A. On the Way to the Web: The Secret History of the Internet and Its Founders. United States of America: Apress, 2008. 215 p.

BARAN, Paul. On Distributed Communications Network. IEEE Transactions of the Professional Technical Group on Communications Systems. [s.l.], p. 1–9. Mar. 1964.

BARNETT, Michael; DUVALL, Raymond. Power in International Politics. International Organization, Cambridge, v. 59, n. 1, p. 39–75, Winter 2005.

BARRATT, Monica J.; LENTON, Simon; ALLEN, Matthew. Internet content regulation, public drug websites and the growth in hidden Internet services. Drugs: Education, Prevention and Policy, [s.l.], v. 20, n. 3, p. 195–202, 12 Dec. 2012.

BECKETT, Andy. The Dark Side of the Internet. 2009. Available at: https://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet. Accessed: 06 Nov. 2017.

BENKLER, Yochai. WikiLeaks and the Protect-IP Act: A new public-private threat to the internet commons. Daedalus: The Journal of the American Academy of Arts and Science, [s.l.], v. 140, n. 4, p. 154–164, Oct. 2011.

BERENGER, Ralph D. Introduction: War in Cyberspace. Journal of Computer-Mediated Communication, [s.l.], v. 12, n. 1, p. 176–188, Oct. 2006.

BERGHEL, Hal. Which Is More Dangerous—the Dark Web or the Deep State? Computer, [s.l.], v. 50, n. 7, p. 86–91, 2017.

BERGMAN, Michael K. White Paper: The Deep Web. The Journal of Electronic Publishing, [s.l.], v. 7, n. 1, p. 1–17, 1 Aug. 2001.

BIDDLE, P. et al. The darknet and the future of content distribution. 2002.

BIRYUKOV, A.; PUSTOGAROV, I.; WEINMANN, R. Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization. 2013 IEEE Symposium on Security and Privacy, [s.l.], p. 80–94, May 2013.

BRADBURY, Danny. Chaos aims to crack China's Wall. The Guardian. London, p. 1–2. 07 Aug. 2008.

BRADBURY, Danny. The problem with Bitcoin. Computer Fraud & Security, [s.l.], v. 2013, n. 11, p. 5–8, Nov. 2013.

BREWSTER, Tom. Simplelocker Android Malware locks up mobile data and demands a ransom. The Guardian. London, p. 1–2. 05 Jun. 2014.

BROOKS, Stephen G.; WOHLFORTH, William. World out of Balance: International Relations and the Challenge of American Primacy. Princeton: Princeton University Press, 2008.

BRUNN, Stanley D. A treaty of Silicon for the treaty of Westphalia? New territorial dimensions of modern statehood. Geopolitics, [s.l.], v. 3, n. 1, p. 106–131, Jun. 1998.

BUCHANAN, Ben. Nobody But Us. Paper, Hoover Institution Press, August 30, 2017.

CANABARRO, Diego Rafael. Governança Global da Internet: Tecnologia, Poder e Desenvolvimento. 2014. 432 f. Thesis (Doctorate) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2014.

CAPORASO, James. The Elusive State: International and Comparative Perspectives. London: Sage Publications, 1989.

CASTELLS, Manuel. The Internet Galaxy: Reflections on the Internet, Business, and Society. New York: Oxford University Press, 2001. 292 p.

CASTELLS, Manuel; CARDOSO, Gustavo (Eds.). A Sociedade em Rede: do conhecimento à ação política; Conferência. Belém (Por): Imprensa Nacional – Casa da Moeda, 2005. 435 p.

CEPIK, Marco; CANABARRO, Diego Rafael; BORNE, Thiago. A Securitização do Ciberespaço e Terrorismo: Uma Abordagem Crítica. In: SOUZA, André de Mello e; NASSER, Reginaldo Mattar; MORAES, Rodrigo Fracalossi de (Eds.). Do 11 de Setembro de 2001 à Guerra ao Terror: Reflexões sobre o Terrorismo no Século XXI. Brasília: IPEA, 2014. Ch. 7. p. 161–186.

CEPIK, Marco; CANABARRO, Diego; BORNE, Thiago. Cyberwar: Clausewitzian Encounters. Space & Defense – USAF Academy, Volume 08, Issue 01, p. 19–33, 2015.

CERUZZI, Paul E. A History of Modern Computing. 2. ed. Cambridge: The MIT Press, 2003. 438 p.

CHAABANE, Abdelberi; MANILS, Pere; KAAFAR, Mohamed. Digging into Anonymous Traffic: a deep analysis of the Tor anonymizing network. In: INTERNATIONAL CONFERENCE ON NETWORK AND SYSTEM SECURITY, 4., 2010, Grenoble. Proceedings. [s.l.]: IEEE Computer Society, 2010. p. 167–174.

CHEN, Hsinchun. Intelligence and Security Informatics for International Security: Information Sharing and Data Mining. New York: Springer, 2006.

CHERTOFF, Michael; SIMON, Tobby. The Impact of the Dark Web on Internet Governance and Cyber Security. London: Centre for International Governance Innovation and Chatham House, 2015. 18 p.

CHOUCRI, Nazli; GOLDSMITH, Daniel. Lost in cyberspace: Harnessing the Internet, international relations, and global security. Bulletin of the Atomic Scientists, [s.l.], v. 68, n. 2, p. 70–77, Mar. 2012.

CHRISTIN, Nicolas. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. [s.l.]: Carnegie Mellon, 2012. 26 p.

CLARKE, Ian. A Distributed Decentralised Information Storage and Retrieval System. 1999. 43 f. Undergraduate thesis – University of Edinburgh, Edinburgh, 1999.

CLARKE, Richard. War from Cyberspace. Georgetown Journal of International Affairs, Washington, D.C., p. 31–36, 2009.

CLAUDE, Inis L. The balance of power revisited. Review of International Studies, Cambridge, v. 2, n. 15, p. 77–85, Apr. 1989.

CLAYTON, Richard; MURDOCH, Steven J.; WATSON, Robert N. M. Ignoring the Great Firewall of China. Privacy Enhancing Technologies, [s.l.], p. 20–35, 2006.

COMPUTER HOPE. Jargon. Available at: https://www.computerhope.com/jargon/p/proxyser.htm. Accessed: 4 Nov. 2017.

CORNISH, Paul et al. On Cyber Warfare. London: The Royal Institute of International Affairs (Chatham House), 2010. 38 p.

CUBRILOVIC, Nik. The Anatomy of the Twitter Attack: Part II. The Washington Post. Washington, 18 Dec. 2009. p. 1–2.

CURRAN, Giorel; GIBSON, Morgan. WikiLeaks, Anarchism and Technologies of Dissent. Antipode, [s.l.], v. 45, n. 2, p. 294–314, 22 May 2012.

DAHL, Robert A. Who Governs?: Democracy and Power in an American City. New Haven: Yale University Press, 1961. 355 p.

DAHL, Robert A. The concept of power. Behavioral Science, [s.l.], v. 2, n. 3, p. 201–215, Jul. 1957.

DEIBERT, Ronald. Divide and Rule: Republican Security Theory as Civil Society Cyber Strategy. Georgetown Journal of International Affairs, Washington, D.C., p. 45–56, 2013.

DEMANT, Jakob; MUNKSGAARD, Rasmus; HOUBORG, Esben. Personal use, social supply or redistribution? Cryptomarket demand on Silk Road 2 and Agora. Trends in Organized Crime, [s.l.], v. 21, n. 1, p. 42–61, 15 Jun. 2016.

DEMCHAK, Chris; DOMBROWSKI, Peter. Cyber Westphalia: Asserting State Prerogatives in Cyberspace. Georgetown Journal of International Affairs, Washington, D.C., p. 29–38, 2013.

DEVINE, Jane; EGGER-SIDER, Francine; ROJAS, Alexandra. The Evolving Impact

of the Invisible Web: Exploring Economic and Political Ramifications. Journal of Web Librarianship, [s.l.], v. 9, n. 4, p. 145–161, 2 Oct. 2015.

DHUNGEL, Prithula et al. Waiting for Anonymity: Understanding Delays in the Tor Network. In: INTERNATIONAL CONFERENCE ON PEER-TO-PEER COMPUTING (P2P), 10., 2010, Delft. Proceedings. [s.l.]: IEEE, 2010. p. 1–4.

DINGLEDINE, Roger; MATHEWSON, Nick; SYVERSON, Paul. Deploying Low-Latency Anonymity: Design Challenges and Social Factors. IEEE Security & Privacy Magazine, [s.l.], v. 5, n. 5, p. 83–87, Sep. 2007.

DINGLEDINE, Roger; MATHEWSON, Nick; SYVERSON, Paul. Tor: The second-generation onion router. In: CONFERENCE ON USENIX SECURITY SYMPOSIUM, 13., 2004, San Diego. Proceedings. Berkeley: USENIX Association, 2004. v. 13, p. 1–17.

DINGLEDINE, Roger; MATHEWSON, Nick. Anonymity Loves Company: Usability and the Network Effect. The Free Haven Project. [s.l.], p. 1–12. Jun. 2006.

EDMAN, Matthew; SYVERSON, Paul. AS-awareness in Tor path selection. Proceedings of the 16th ACM Conference on Computer and Communications Security – CCS '09, [s.l.], p. 380–389, 2009.

ELAHI, Tariq et al. Changing of the Guards: a framework for understanding and improving entry guard selection in Tor. Proceedings of the 2012 ACM Workshop on Privacy in the Electronic Society. Raleigh, p. 43–54. 15 Oct. 2012.

ENSAFI, Roya et al. Examining How the Great Firewall Discovers Hidden Circumvention Servers. Proceedings of the 2015 ACM Conference on Internet Measurement Conference – IMC '15, [s.l.], p. 445–458, 2015.

EUROPEAN COUNCIL FOR NUCLEAR RESEARCH (Switzerland) (Ed.). About CERN. 2017. Available at: https://home.cern/about. Accessed: 22 Sep. 2017.

EVERETT, Cath. Moving Across to the Dark Side. Network Security. [s.l.], Sep. 2009. p. 10–12.

FARRELL, Henry. Regulating Information Flows: States, Private Actors, and E-Commerce. Annual Review of Political Science, [s.l.], v. 9, n. 1, p. 353–374, Jun. 2006.

FARRELL, Henry. Why 'Dark Web' drug markets will keep on imploding. The Washington Post. Washington, p. 1–4. 19 Mar. 2015.

FIFIELD, David et al. Evading Censorship with Browser-Based Proxies. In: PRIVACY ENHANCING TECHNOLOGIES SYMPOSIUM, 12., 2012, Vigo. Proceedings. Berlin: Springer-Verlag, 2012. p. 1–20.

FINKLEA, Kristin. Dark Web. Washington D.C.: CRS Report, 2015. 15 p.

FREE HAVEN$_a$. Home. 2017. Available at: https://www.freehaven.net/index.html. Accessed: 24 Nov. 2017.

FREE HAVEN$_b$. Overview. 2017. Available at: https://www.freehaven.net/overview.html. Accessed: 24 Nov. 2017.

FREENET. About. 2017. Available at: https://freenetproject.org/pages/about.html. Accessed: 16 Nov. 2017.

FOUCAULT, Michel. The Subject and Power. Critical Inquiry, Chicago, v. 8, n. 4, p. 777–795, Summer 1982.

FOX-BREWSTER, Tom. Silk Road 2.0 targeted in 'Operation Onymous' dark web takedown. The Guardian. London, p. 1–5. 07 Nov. 2014.

FOX-BREWSTER, Tom. Facebook opens up to anonymous Tor users with .onion address. The Guardian. London, p. 1–3. 31 Oct. 2014.

GARDNER, Joshua. Anonymous online marketplace that replaced Silk Road VANISHES... taking $100MILLION of users' money with it. Daily Mail. London, p. 1–6. 03 Dec. 2013.

GEHL, Robert W. Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. New Media & Society, [s.l.], v. 18, n. 7, p. 1219–1235, 15 Oct. 2014.

GHAPPOUR, Ahmed. Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web. Stanford Law Review. Stanford, p. 1075–1136. Apr. 2017.

GUZZINI, Stefano. The Use and Misuse of Power Analysis in International Theory. In: PALAN, Ronen (Ed.). Global Political Economy: Contemporary Theories. London: Routledge, 2000. p. 53–66.

HACKL, Andrea M.; BECKER, Amy B.; TODD, Maureen E. "I Am Chelsea Manning": Comparison of Gendered Representation of Private Manning in U.S. and International News Media. Journal of Homosexuality, [s.l.], v. 63, n. 4, p. 467–486, 31 Aug. 2015.

HALLONSTEN, Olof. The Politics of European Collaboration in Big Science. Global Power Shift, [s.l.], p. 31–46, 2014.

HATHAWAY, Melissa E. Leadership and Responsibility for Cybersecurity. Georgetown Journal of International Affairs, Washington, D.C., p. 71–80, 2012.

HE, Bin et al. Accessing the Deep Web: Attempting to Locate and Quantify Material on the Web that is Hidden from Typical Search Techniques. Communications of the ACM, [s.l.], v. 50, n. 5, p. 94–101, Apr. 2007.

HENDEL, Charles W. David Hume's Political Essays. Indianapolis: Bobbs-Merrill, 1953.

HERN, Alex. New ransomware employs Tor to stay hidden from security. The Guardian. London, p. 1–2. 25 Jul. 2014.

HERN, Alex. US Defence Department funded Carnegie Mellon research to break Tor. The Guardian. London, p. 1–2. 25 Feb. 2016.

HOOD, Christopher. From FOI World to WikiLeaks World: A new chapter in the transparency story? Governance: An International Journal of Policy, Administration and Institutions, [s.l.], v. 24, n. 4, p. 635–638, Oct. 2011.

HOPF, Ted. The Promise of Constructivism in International Relations Theory. International Security, Cambridge, v. 23, n. 1, p. 171–200, Summer 1998.

HOPPER, Nicholas; VASSERMAN, Eugene Y.; CHAN-TIN, Eric. How much anonymity does network latency leak? ACM Transactions on Information and System Security, [s.l.], v. 13, n. 2, p. 1–28, 1 Feb. 2010.

HORSMAN, Graeme. Can we continue to effectively police digital crime? Science & Justice, [s.l.], v. 57, n. 6, p. 448–454, Nov. 2017.

HURWITZ, Roger. Keeping Cool: steps for avoiding conflict and escalation in Cyberspace. Georgetown Journal of International Affairs, Washington, D.C., p. 17–28, 2013.

JAJODIA, Sushil et al. Cyber Warfare: Building the Scientific Foundation. Switzerland: Springer, 2015. 321 p.

JOHNSON, Aaron et al. Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries. In: ACM SIGSAC CONFERENCE ON COMPUTER & COMMUNICATIONS SECURITY, 13., 2013, Berlin. Proceedings. New York: ACM, 2013. p. 337–348.

JOUVENEL, Bertrand de. Sovereignty: An Inquiry into the Political Good. Chicago: University of Chicago Press, 1957.

JUNIO, Timothy J. How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate. Journal of Strategic Studies, [s.l.], v. 36, n. 1, p. 125–133, Feb. 2013.

KALLBERG, Jan; THURAISINGHAM, Bhavani. Towards cyber operations: the new role of academic cyber security research and education. 2012 IEEE International Conference on Intelligence and Security Informatics, [s.l.], p. 132–134, Jun. 2012.

KAUFMANN, Stuart J.; LITTLE, Richard; WOHLFORTH, William C. (Ed.). The Balance of Power in World History. London: Palgrave Macmillan, 2007.

KEOHANE, Robert O.; NYE, Jr. Joseph S. Power and Interdependence. 4. ed. [s.l.]: Longman, 2011. 330 p.

KIRK, Jeremy. Researcher intercepted embassy passwords. Washington Post. Washington, 10 Sep. 2007. p. 1–2.

KRAMER, Franklin D. Achieving International Cyber Stability. Georgetown Journal of International Affairs, Washington, D.C., p. 121–137, 2012.

KRIGE, John; BARTH, Kai-Henrik. Introduction. Osiris, [s.l.], v. 21, n. 1, p. 1–21, Jan. 2006.

LAKSHMAN, T. V.; MADHOW, Upamanyu. The Performance of TCP/IP for Networks with High Bandwidth-Delay Products and Random Loss. IEEE/ACM Transactions on Networking, [s.l.], v. 5, n. 3, p. 336–350, Jun. 1997.

LASSWELL, Harold D.; KAPLAN, Abraham. Power and Society: A Framework for Political Inquiry. New Haven: Yale University Press, 1950.

LAWSON, Sean. Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States. First Monday, [s.l.], v. 17, n. 7, p. 1–17, 2 Jul. 2012.

LEE, Micah. Edward Snowden explains how to reclaim your privacy. 2015. Available at: https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy/. Accessed: 07 Dec. 2016.

LI, Bingdong et al. An Analysis of Anonymizer Technology Usage. Traffic Monitoring and Analysis, [s.l.], p. 108–121, 2011.

LIBICKI, Martin C. Cyberdeterrence and Cyberwar. Santa Monica: RAND Corporation, 2009. 214 p.

LITTLE, Richard. The Balance of Power in International Relations: Metaphors, Myths and Models. Cambridge: Cambridge University Press, 2007.

LOESING, Karsten; MURDOCH, Steven J.; DINGLEDINE, Roger. A Case Study on Measuring Statistical Data in the Tor Anonymity Network. Financial Cryptography and Data Security, [s.l.], p. 203–215, 2010.

LUKES, Steven. Power: A Radical View. 2. ed. London: Palgrave Macmillan, (1974), 2005.

MADDOX, Alexia et al. Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde'. Information, Communication & Society, [s.l.], v. 19, n. 1, p. 111–126, 15 Oct. 2015.

MANJIKIAN, Mary McEvoy. From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. International Studies Quarterly, [s.l.], v. 54, n. 2, p. 381–401, 7 Jun. 2010.

MARTIN, James. Lost on the Silk Road: Online drug distribution and the 'cryptomarket'.

Criminology & Criminal Justice, [s.l.], v. 14, n. 3, p. 351–367, 7 Oct. 2013.

MASONI, Marco; GUELFI, Maria Renza; GENSINI, Gian Franco. Darknet and bitcoin, the obscure and anonymous side of the internet in healthcare. Technology and Health Care, [s.l.], v. 24, n. 6, p. 969–972, 14 Nov. 2016.

MATHEWS, Jessica T. Power Shift. Foreign Affairs, [s.l.], v. 76, n. 1, p. 50–66, 1997.

McCOY, Damon et al. Shining Light in Dark Places: Understanding the Tor Network. In: PRIVACY ENHANCING TECHNOLOGIES SYMPOSIUM, 2008, [s.l.]. Proceedings. Berlin: Springer-Verlag, 2008. v. 5134, p. 63–76.

MEARSHEIMER, John J. The Tragedy of Great Power Politics. New York: W. W. Norton, 2001.

MICHALSKI, Milena; GOW, James. War, Image and Legitimacy: Viewing contemporary conflict. New York: Routledge, 2007.

MILLS, John R. The Key Terrain of Cyber. In: McGANN, Nora; HANDEL, William (Ed.). International Engagement on Cyber: Establishing Norms and Improving Security. Washington, D.C.: Georgetown Journal of International Affairs, 2012. p. 99–108.

MITTAL, Prateek et al. Stealthy Traffic Analysis of Low-Latency Anonymous Communication Using Throughput Fingerprinting. In: ACM WORKSHOP ON PRIVACY IN THE ELECTRONIC SOCIETY, 18., 2011, [s.l.]. Proceedings. Chicago: ACM, 2011. p. 215–226.

MOGHADDAM, Hooman Mohajeri et al. SkypeMorph: Protocol Obfuscation for Tor Bridges. In: ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 12., 2012, Raleigh. Proceedings. [s.l.]: ACM, 2012. p. 97–108.

MONTEIRO, Silvana Drumond; FIDENCIO, Marcos Vinicius. As Dobras Semióticas do Ciberespaço: da Web Visível à Invisível. Transinformação, Campinas, v. 25, n. 1, p. 35–46, Apr. 2013.

MOORE, Daniel; RID, Thomas. Cryptopolitik and the Darknet. Survival, [s.l.], v. 58, n. 1, p. 7–38, 2 Jan. 2016.

MORGENTHAU, Hans J. Politics Among Nations: The Struggle for Power and Peace. New York: Alfred A. Knopf Inc., 1948. 516 p.

MOUL, William B. Measuring the 'Balances of Power': a look at some numbers. Review of International Studies, Cambridge, v. 2, n. 15, p. 101–121, Apr. 1989.

MOYER, Justin. With Tor, Facebook is first social media giant to venture into the 'dark Web'. The Washington Post. London, p. 1–2. 04 Nov. 2014.

MUELLER, Milton; SCHMIDT, Andreas; KUERBIS, Brenden. Internet Security and

Networked Governance in International Relations. International Studies Review, [s.l.], v. 15, n. 1, p. 86–104, Mar. 2013.

NAGEL, Jack H. The Descriptive Analysis of Power. New Haven: Yale University Press, 1975.

NAUGHTON, John. A Brief History of the Future: The Origins of the Internet. Great Britain: Weidenfeld & Nicolson, 1999.

NISSENBAUM, Helen. Where Computer Security Meets National Security. Ethics and Information Technology, [s.l.], v. 7, n. 2, p. 61–73, Jun. 2005.

NYE, Joseph S. Cyber Power. Cambridge: Belfer Center for Science and International Affairs, 2010. 24 p.

NYE, Joseph S. The Future of Power. New York: Public Affairs, 2011.

NYE, Joseph S. The Regime Complex for Managing Global Cyber Activities. Cambridge: Belfer Center for Science and International Affairs, 2014. 20 p.

PACE, Jonathan. Exchange relations on the dark web. Critical Studies in Media Communication, [s.l.], v. 34, n. 1, p. 1–13, 17 Oct. 2016.

PAGE, Mark; SPENCE, J. E. Open Secrets Questionably Arrived At: The Impact of WikiLeaks on Diplomacy. Defence Studies, [s.l.], v. 11, n. 2, p. 234–243, Jun. 2011.

PANCHENKO, Andriy; PIMENIDIS, Lexi; RENNER, Johannes. Performance Analysis of Anonymous Communication Channels Provided by Tor. 2008 Third International Conference on Availability, Reliability and Security, [s.l.], p. 221–228, Mar. 2008.

PAQUET-CLOUSTON, Masarah; DÉCARY-HÉTU, David; MORSELLI, Carlo. Assessing market competition and vendors' size and scope on AlphaBay. International Journal of Drug Policy, [s.l.], v. 54, p. 87–98, Apr. 2018.

PAUL, T. V. Introduction: The Enduring Axioms of Balance of Power Theory and Their Contemporary Relevance. In: PAUL, T. V.; WIRTZ, James J.; FORTMANN, Michel. Balance of Power: Theory and Practice in the 21st Century. Stanford: Stanford University Press, 2004. Introduction. p. 1–25.

PETERSON, Andrea. A bunch of Tor sites spread malware: Was the FBI behind it? The Washington Post. Washington, p. 1–2. 05 Aug. 2013.

PHELPS, Amy; WATT, Allan. I shop online – recreationally! Internet anonymity and Silk Road enabling drug use in Australia. Digital Investigation, [s.l.], v. 11, n. 4, p. 261–272, Dec. 2014.

PILKINGTON, Ed. Chelsea Manning released from military prison. The Guardian. London, p. 1–3. 17 May 2017.

POLLARD, A. F. The Balance of Power. Journal of the British Institute of International Affairs, Princeton, v. 2, n. 2, p. 51–64, Mar. 1923.

PORTER, Brian (Ed.). The Aberystwyth Papers: International Politics 1919–1969. Oxford: Oxford University Press, 1972.

POWER, Mike. Life After the Silk Road: How the darknet drugs market is booming. The Guardian. London, p. 1–4. 30 May 2014.

PRIGG, Mark; PRESS, Associated. Silicon Valley software engineer, 26, arrested for 'setting up Silk Road style drug-dealing site'. Daily Mail. London, p. 1–6. 06 Nov. 2014.

RIFFE, Daniel; LACY, Stephen; FICO, Frederick G. Analyzing Media Messages: Using Quantitative Content Analysis in Research. 2. ed. London: Lawrence Erlbaum Associates, 2008. 251 p.

ROCHE, Edward M. Information and Communication Technology Still a Force for Good? Journal of Global Information Technology Management, [s.l.], v. 19, n. 2, p. 75–79, 2 Apr. 2016.

ROCHE, Edward M.; BLAINE, Michael J. International Convention for the Peaceful Use of Cyberspace. Orbis, [s.l.], v. 58, n. 2, p. 282–296, 2014.

RON, Dorit; SHAMIR, Adi. How did Dread Pirate Roberts Acquire and Protect his Bitcoin Wealth. In: INTERNATIONAL CONFERENCE ON FINANCIAL CRYPTOGRAPHY AND DATA SECURITY, 18., 2014, Christ Church. Proceedings. Israel: The Weizmann Institute of Science, 2014. v. 8438, p. 3–15.

ROSS, Alec. Digital Diplomacy and US Foreign Policy. The Hague Journal of Diplomacy, [s.l.], v. 6, n. 3, p. 451–455, 1 Jan. 2011.

ROTHE, Dawn L.; STEINMETZ, Kevin F. The case of Bradley Manning: state victimization, realpolitik and WikiLeaks. Contemporary Justice Review, [s.l.], v. 16, n. 2, p. 280–292, Jun. 2013.

RUSHE, Dominic. Silk Road 2.0's alleged owner arrested as drugs website shuttered by FBI. The Guardian. London, p. 1–5. 06 Nov. 2014.

SANDVIK, Runa. The New York Times is Now Available as a Tor Onion Service. 2017. Available at: https://open.nytimes.com/https-open-nytimes-com-the-new-york-times-as-a-tor-onion-se Accessed: 5 Dec. 2017.

SCHMIDT, Brian C. On the History and Historiography of International Relations. In: CARLSNAES, Walter; RISSE, Thomas; SIMMONS, Beth A. (Ed.). Handbook of International Relations. 2. ed. London: Sage Publications Ltd, 2013. Ch. 1. p. 3–28.

SCHNEIDER, Jacquelyn. Digitally-enabled Warfare: the Capability-Vulnerability Para-

dox. Washington: Center for a New American Security, 2016. 11 p.

SCHREIER, Fred. On Cyberwarfare. 7. ed. Geneva: The Geneva Centre for the Democratic Control of Armed Forces, 2015. 132 p.

SCHULZE, Matthias. Clipper Meets Apple vs. FBI—A Comparison of the Cryptography Discourses from 1993 and 2016. Media and Communication, [s.l.], v. 5, n. 1, p. 54–62, 22 Mar. 2017.

SCHWELLER, Randall L. Unanswered Threats: Political Constraints on the Balance of Power. Princeton: Princeton University Press, 2006.

SHEEHAN, Michael. The Balance of Power: History & Theory. London, New York: Routledge, 1996. 229 p.

SHERMAN, Chris; PRICE, Gary. The Invisible Web: Uncovering Information Sources Search Engines Can't See. 2. ed. Medford: CyberAge Books, 2001. 450 p.

SIEDLER, Ragnhild Endresen. Hard Power in Cyberspace: CNA as a Political Means. In: INTERNATIONAL CONFERENCE ON CYBER CONFLICT, 8., 2016, Tallinn. Proceedings. Tallinn: Council of Europe Publications, 2016. p. 23–36.

SIMONDS, F. R.; EMENY, B. The Great Powers in World Politics. New York: American Book, 1937.

SKOLNIKOFF, Eugene B. The Elusive Transformation: Science, Technology and the Evolution of International Politics. Princeton: Princeton University Press, 1993. 322 p.

STRANGE, Susan. States and Markets. London: Continuum, 1988. 265 p.

STRANGE, Susan. The Retreat of the State: The Diffusion of Power in the World Economy. Cambridge: Cambridge University Press, 1996. 218 p.

TECH TERMS$_a$. The Tech Terms Computer Dictionary. 2017. Available at: https://techterms.com/definition/script. Accessed: 02 Dec. 2017.

TECH TERMS$_b$. The Tech Terms Computer Dictionary. 2017. Available at: https://techterms.com/definition/relational_database. Accessed: 02 Dec. 2017.

THOMSON, Iain. Dark web doesn't exist, says Tor's Dingledine. And folks use network for privacy, not crime. 2017. Available at: https://www.theregister.co.uk/2017/07/29/tor_dark_web/. Accessed: 29 Oct. 2017.

TIKK-RINGAS, Eneken. The Implication of Mandates in International Cyber Affairs. In: McGANN, Nora; HANDEL, William (Ed.). International Engagement on Cyber: Establishing Norms and Improving Security. Washington, D.C.: Georgetown Journal of International Affairs, 2012. p. 99–108.

TOR PROJECT. Projects. Available at: https://www.torproject.org/projects/projects.

html.en. Accessed: 21 Nov. 2017.

TZANETAKIS, Meropi. Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time. International Journal of Drug Policy, [s.l.], v. 56, p. 176–186, Jun. 2018.

VAISHNAV, Chintan; CHOUCRI, Nazli; CLARK, David. Cyber international relations as an integrated system. Environment Systems and Decisions, [s.l.], v. 33, n. 4, p. 561–576, 17 Nov. 2013.

VAN HOUT, Marie Claire; BINGHAM, Tim. Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. International Journal of Drug Policy, [s.l.], v. 25, n. 2, p. 183–189, Mar. 2014.

VITALIEV, Dmitri. Vaulting the great Firewall. The Guardian. London, p. 1–2. 05 Aug. 2008.

WALSH, Lucas; BARBARA, Julien. Speed, International Security, and. Journal of Computer-Mediated Communication, [s.l.], v. 12, n. 1, p. 189–208, Oct. 2006.

WALT, Stephen M. The Origins of Alliances. London: Cornell University Press, 1987.

WALTZ, Kenneth N. Theory of International Politics. London: Addison-Wesley, 1979.

WALTZ, Kenneth N. Realist Thought and Neorealist Theory. Journal of International Affairs, [s.l.], v. 1, n. 44, p. 21–38, Summer 1990.

WEBER, Max. The Theory of Social and Economic Organization. New York: Oxford University Press, 1947. 436 p.

WEISS, Charles. Science, technology and international relations. Technology in Society, [s.l.], v. 27, n. 3, p. 295–313, Aug. 2005.

WENDT, Alexander. Anarchy is What the States Make of it: The Social Construction of Power Politics. International Organization, [s.l.], v. 46, n. 2, p. 391–425, Spring 1992.

WENDT, Alexander. Social Theory of International Politics. Cambridge: Cambridge University Press, 1999.

WIKILEAKS (Ed.). Featured. 2016. Available at: https://wikileaks.org/. Accessed: 08 Sep. 2016.

WRIGHT, Quincy. The Study of International Relations. New York: Appleton-Century-Crofts, 1955.

WRIGHT, Quincy. A Study of War: Volume I. Chicago: University of Chicago Press, 1942.

WRIGHT, Quincy. A Study of War: Volume II. Chicago: University of Chicago Press,

1942.

ZULKARNINE, Ahmed T. et al. Surfacing collaborated networks in dark web to find illicit and criminal content. 2016 IEEE Conference on Intelligence and Security Informatics (ISI), [s.l.], p. 109–114, Sep. 2016.

Annexes

Annex 1 – Representative Pyramid of Structural Power

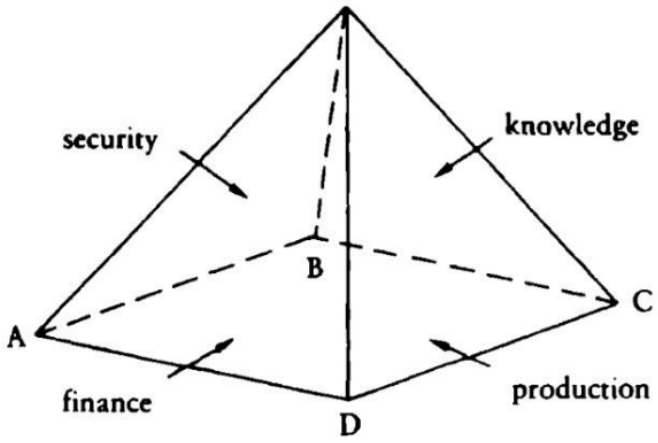


Figure: Representative pyramid of structural power showing the four primary structures: Security, Production, Finance, and Knowledge.

Source: STRANGE, 1988, p.27.

Annex 2 – Physical and Virtual Dimensions of Cyber Power

Table 1: Physical and Virtual Dimensions of Cyber Power

	Targets of Cyber Power	
	Intra cyber space	**Extra cyber space**
Information Instruments	Hard: Denial of service attacks Soft: Set norms and standards	Hard: Attack SCADA systems Soft: Public diplomacy campaign to sway opinion
Physical Instruments	Hard: Government controls over companies Soft: Infrastructure to help human rights activists	Hard: Bomb routers or cut cables Soft: Protests to name and shame cyber providers

Figure: Physical and virtual dimensions of cyber power.

Source: NYE, 2010, p.5.

Annex 3 – Distributed Network

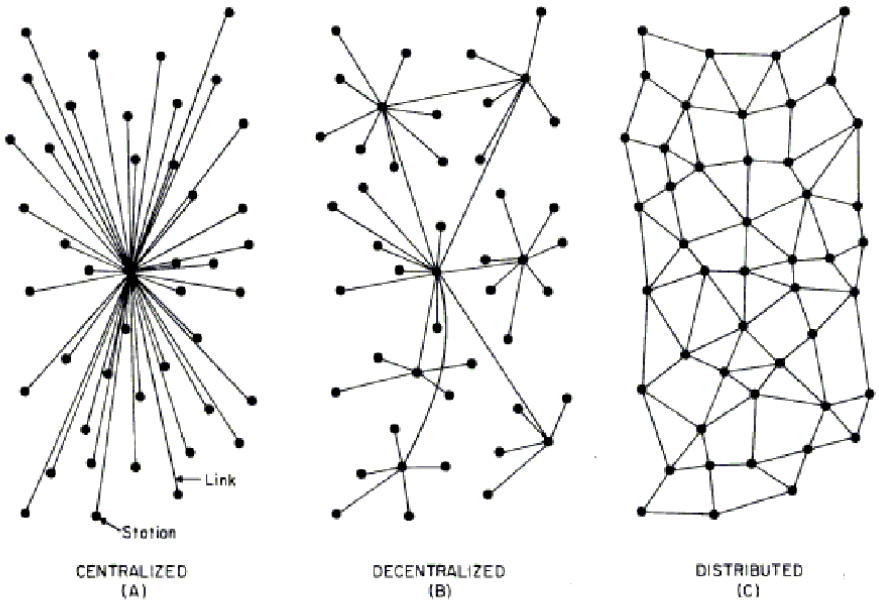


FIG. 1 — Centralized, Decentralized and Distributed Networks

Figure: Paul Baran's distributed network topology compared to centralized and decentralized networks.

Source: BARAN, 1964, p.2.

Annex 4 – Data Traffic Volume by Protocol on the "NFS Internet Backbone"

Date	% ftp	% telnet	% netnews	% ire	% gopher	% email	% web
Mar.93	42.9	5.6	9.3	1.1	1.6	6.4	0.5
Dec.93	40.9	5.3	9.7	1.3	3.0	6.0	2.2
Jun.94	35.2	4.8	10.9	1.3	3.7	6.4	6.1
Dec.94	31.7	3.9	10.9	1.4	3.6	5.6	16.0
Mar.95	24.2	2.9	8.3	1.3	2.5	4.9	23.9

Figure: Data traffic volume by protocol on the NFS Internet Backbone.

Source: NAUGHTON, 1999, p.248.

Annex 5 – The Various Webs

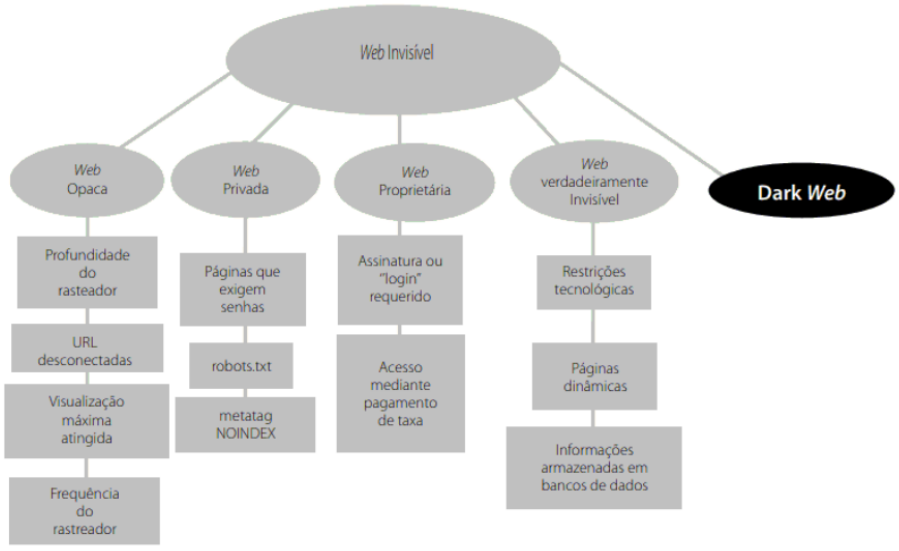


Figura 2. As várias *Web*.

Figure: Classification of the various layers of the web.

Source: FIDÊNCIO; MONTEIRO, 2013, p.41.

Annex 6 – "Directly Connecting Users"

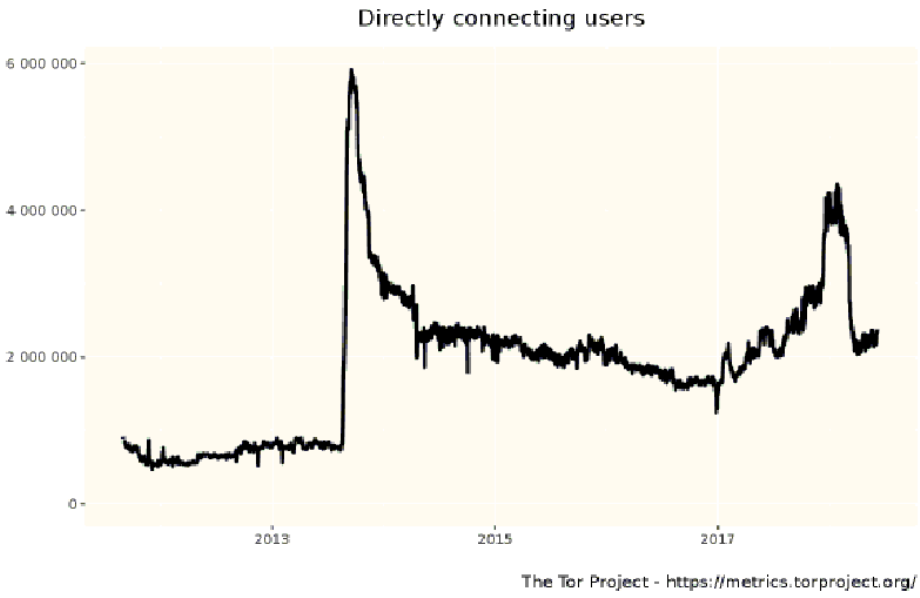


Figure: Number of directly connecting Tor users over time.

Source: THE TOR PROJECT, 2018 (metrics.torproject.org).

Annex 7 – Classification

Category	Websites
None	2,482
Other	1,021
Drugs	423
Finance	327
Other illicit	198
Unknown	155
Extremism	140
Illegitimate pornography	122
Nexus	118
Hacking	96
Social	64
Arms	42
Violence	17
Total	5,205
Total active	2,723
Total illicit	1,547

Figure: Classification of content found on Tor hidden services.

Source: MOORE; RID, 2016, p.21.

Appendices

Appendix 1 – To Be an Authority

Excerpts from *The Retreat of the State: The Diffusion of Power in the World Economy* by Susan Strange, 1996.

Page	Quote
p.xiii	The implicit assumption conveyed by the two words, 'global' and 'governance', is that government is being achieved on a world scale by a world **authority**.
p.xv	I firmly believe that the new realism of the Stopford-Strange analysis of corporate strategies and state development policies makes it imperative to look seriously at the power exercised by **authorities** other than states.
p.115	Representatives of the Italian state in Rome began to think better of their delegation of **authority** to the mafia as the latter tended to act more and more blatantly outside the law. A new generation of well-trained magistrates, themselves mostly Sicilians, were courageous enough to initiate an open break between state and mafia.
p.116	Sociologists have argued that criminal gangs, like underground resistance movements in wartime or recalcitrant groups in prisons, tend to emerge when state **authority**, for whatever reason is already weakened, and the government has lost or failed to obtain the consent of the governed.
p.165	Here, we must distinguish between functions and **authority** that are consciously delegated to the organisation by member states, and functions and **authority** that have been assumed by the officials, independently of the wishes or decisions of member states.

Page	Quote
p.168	The net result of leaving each creditor to define the terms and modalities of debt relief was that **authority** was delegated on a case-by-case basis to international institutions other than the United Nations or the IMF or IBRD — the so-called Paris Club or official creditors and the London Club of private creditors. There are other less politically important matters on which member states have delegated executive **authority** — or seemed to do so — to international institutions.
p.171	Four major examples show that such delegation is conceded only when the system — some part of the structures of the world market economy — is perceived as being seriously at risk, and when the direct and indirect costs of delegated **authority** are relatively insignificant. Here we may ignore the Council of Ministers, as being clearly an inter-governmental body whose members are named by and responsible to national governments. It is only important insofar as it delegates **authority** to the Commission, to the Parliament or to the European Court, independent of national governments.
p.173	Whether this trend in Europe is peculiar to the European Community or is a harbinger of a more general shift of **authority** to international judicial bodies is a much more open question.
p.174	Although German resistance on behalf of national regulatory **authority** stopped the complete transfer of **authority** over mergers to the EC, some significant shift did take place.
p.179	Transfer of **authority** from the member governments to federal institutions over this central responsibility of political **authority** in a market economy has not yet happened.
p.187	Another feature which the triangular model also accommodates is the fact that there are striking variations across sectors in the nature and kind of **authority** and how much it, or they, intervene with the play of market forces.
p.189	Mine's argument in *Le Nouveau Moyen Age* is that these areas without legitimate, acknowledged **authority**, in which the law of the jungle rules, are growing, especially in Africa and in the former Soviet Union. **authority** is divided between the formal institutions of the state and local potentates, chiefs or gang leaders; between vassal and suzerain, the responsibility for keeping order is as unclear as it was in the middle ages.
p.192	Although there were occasions when the delegation of **authority** to an international institution, as to any other body, seemed to give it some independent power of its own, that was usually more an illusion than reality.

Page	Quote
p.198	To make **authority** acceptable, effective and respected, there has to be some combination of forces to check the arbitrary or self-serving use of power and to see that it is used at least in part for the common good.

Source: STRANGE, 1996.

Appendix 2 – To Exercise Authority

Excerpts from *The Retreat of the State: The Diffusion of Power in the World Economy* by Susan Strange, 1996.

Page	Quote
p.110	For example, its **authority** — like that of a state — is exercised through an established power structure, by means of which obedience is rewarded and disobedience punished, occasionally by the use of violence and always by the threat of violence.
p.133	[...] **authority** in political economy is recognisable by the power to alter or modify the behaviour of others by using incentives and disincentives to affect the choice and range of options, [...]
p.171	The conclusion must be that IOs, both in their dependent and independent exercise of **authority**, are essentially system-preserving.
p.184	The first, basic question was 'Who, or what, is responsible for change?' The second was 'Who, or what, exercises **authority** — the power to alter **outcomes** and redefine options for others — in the world economy or world society?'
p.196	The only other important consequences of the retreat of the state and the diffusion of state **authority** sketched in earlier chapters relates to legitimacy and democracy.
p.197	But if those institutions are now suffering the kind of diffusion of **authority** I have described, not much remains of the accountability of market forces to political constraints. Moreover, none of the non-state **authorities** to whom **authority** has shifted, is democratically governed. Firms — the new players in transnational economic diplomacy — are hierarchies, not democracies.

Page	Quote
p.199	With the end of the Cold War, and with the triumph of the market economy, there is a new absence of absolutes. In a world of multiple, diffused **authority**, each of us shares Pinocchio's problem; our individual consciences are our only guide.

Source: STRANGE, 1996.

Appendix 3 – Control, 1988

Excerpts on **control** in *States and Markets* by Susan Strange, 1988.

Page	Quote	Object
p.30	But finance — the **control** of credit — is the facet which has perhaps risen in importance in the last quarter century more rapidly than any other and has come to be of decisive importance in international economic relations and in the competition of corporate enterprises.	Credit
p.32–33	But the power of the ayatollahs in defending and promoting Islamic virtues would have been constrained if they had not also gained **control** over the state and the armed forces sufficient to confirm their **authority** both within the country and beyond.	State and armed forces
p.37	Too often, they have ignored or refused to contemplate structural power, or the power to define the structure, to choose the game as well as to set the rules under which it is to be played. It is as if you said, 'This man has power in relation to this woman because he can knock her down', ignoring the fact of structural power in a masculine-dominated social structure that gives the man social status, legal rights and **control** over the family money that makes it unnecessary even to threaten to knock her down unless she does as she is told.	Family money

Page	Quote	Object
p.84	The justice or injustice of the distributional effects of change in the production structure in short has been uneven, complex and subjective. Some wider issues concerning the system in general remain to be considered. Among these, there are three, of which the first — whether states have the power to **control** the transnational corporations — is familiar to most people and has been much discussed.	Transnational corporations
p.85	At the national level, the developing states that wanted to have the mandatory 'shall' instead of the advisory 'should' put into a UN Code were meanwhile seeking to use national political power against the foreign corporations. [...] the displaced companies kept **control** over market access, by making long-term contracts with the customers, for instance. They also had command of the technology necessary to remain competitive in world markets.	Market access
p.86	The question now is whether this traditionally exclusive power claimed by all states alike is being eroded by large corporations through their **control** over the production structure.	Production structure
p.101	And there was one final factor that allowed the steady outflow of British capital before 1914 to help the world economy to grow reasonably steadily. It was India. [...] But Britain's political **control** over India allowed London to extract annual shipments of gold in respect of Home Charges and to use its **control** over the sterling-rupee exchange rate and other devices to stop the gold seeping back to the Indian economy.	India / Sterling-rupee exchange rate
p.106	Briefly, the Eurodollar market (and later markets for Eurosterling, Euromarks, Euroyen, etc.) developed because of two inviting gaps in government **controls** over the power of banks to create credit.	Power of banks to create credit

Page	Quote	Object
p.123	In the knowledge structure of medieval Christendom in Europe, beliefs placed a high value on the knowledge of how men and women might achieve eternal salvation. [...] That power and **authority** was reinforced by **control** over the means of communication, in the form of sacred books and of literacy in a common sacred language, Latin.	Means of communication
p.125	Aided by differences of language, national governments could use technology to keep **control** by censorship, by monopoly or by restrictive licensing over national systems of education, over national newspapers and broadcasting and even over the publication of books and periodicals. Thus, in this new knowledge structure, the **authority** of the Church was displaced by the extended **authority** of the scientific state.	National systems of education / national newspapers and broadcasting / publication of books and periodicals
p.128–129	In the Manhattan Project, the US government brought together an international team of top physicists from various countries. But it reserved to itself exclusive **control** over their discovery of how to apply the principles of nuclear fission to warfare.	Discovery of how to apply the principles of nuclear fission to warfare
p.134	The politically important point about these communication systems is, of course, that the bank's head office becomes the gatekeeper, **controlling** access to the system.	Access to the system
p.134	Walter Wriston, former head of Citibank (now Citicorp), has even suggested that 'banking today is information' (Wriston, 1986). Similarly, it is the **control** over, and access to, these global systems that also allows the great grain and commodity trading companies to enjoy such an oligopolistic position as compared with either the producers (the farmers) or the end-users.	Global systems
p.135	But what is important is that now even the systems reserved to the Pentagon depend on, and could not operate without, the technical know-how and co-operation of the major transnational corporations. The possibility of total **control** and monopoly by the state (outside the Soviet Union and China) has seemingly gone for good.	Systems reserved to the Pentagon

Page	Quote	Object
p.155	Like sea transport, the way in which the global air transport system is structured rests on a political fiction: the notion that a state '**controls**' the airspace above its territory, in the same way that, from the eighteenth century until the second half of the twentieth century, it notionally **controlled** its 'territorial waters'. [...] The notion that any government can **control** what goes on in the air above it is obviously even more of a fiction than the notion that it can **control** what goes on in the seas around it.	Airspace / territorial waters
p.188	The United States has dominated and directed the negotiations in the GATT, [...] partly because of the bargaining power conferred on it by its **control** over so large and rich a domestic market.	Domestic market
p.193	But the reason why the European Coal and Steel Community no longer held centre stage by the 1970s was much more economic than political. [...] all the European states no longer **controlled** within their own frontiers their chief source of industrial energy, but were all in the same boat as net importers of oil and gas.	Source of industrial energy
p.202	The Iranian revolution of 1978–9, tempted the OPEC members to try the same gambit again [...] OPEC found itself obliged to agree on a climb-down, a $5 reduction in oil prices by which it hoped to show it was still in **control**. But, this time, the market took charge.	Oil market
p.202	The companies still had **control** of the technology of exploration, of offshore production, of refining and marketing; and they had the capital necessary for risk-taking in an essentially risky business.	Technology of exploration, offshore production, refining, marketing, capital
p.237	[...] the United States has not in fact lost power in the world market economy. As that economy has grown and spread, the source of its power has shifted from the land and the people into **control** over structures of the world system.	Structures of the world system

Page	Quote	Object
p.242	[...] the Americans reserved to themselves the right to decide unilaterally when to abandon sanctions and to use force against Saddam Hussein, and then to decide on the conduct of Desert Storm, and on how and when to call off the attack. Confidence in US leadership has also been undermined, not by a loss of power over others, but by lost **control** over its own tangled web of overblown bureaucracy.	Bureaucracy

Source: STRANGE, 1988.

Appendix 4 – Control, 1996

Excerpts on **control** in *The Retreat of the State: Diffusion of Power in the World Economy* by Susan Strange, 1996.

Page	Quote	Object
p.100	At the peak of their power over society, states claimed, and exercised, the right to **control** the substance of information — by censorship, for example, of books or the press — and to **control** the means by which information was communicated — post, telegraph and telephone.	Substance of information / post, telegraph and telephone
p.100	Other governments have been forced by a combination of technological and economic change to give up their exclusive **control** for the sake of maintaining the competitiveness in world markets of the national economies for whose welfare they are held responsible.	Substance of information / post, telegraph and telephone

Page	Quote	Object
p.105–106	The power of governments which, for social policy reasons, might want to keep rural areas and lonely old people fully integrated into the communications system at minimal costs has clearly diminished. So has the **control** of governments. By means of their ownership of state monopolies, PTTs used to have **control** over the design and availability of such communications. No longer. [...] Even the government of a country with a potential market as large as that of China no longer has the option of **controlling** and running its own communication system; the range of options open to it has narrowed to picking the foreign partners and negotiating with them the best terms of the alliance.	Post, telegraph and telephone (PTTs) / design, availability of PTTs communications
p.108	In telecommunications, the balance of benefit in the last two decades of the twentieth century would seem to have gone to the private sector firms at the expense of governments and their publicly owned and **controlled** enterprises.	Telecommunications enterprises
p.112	One estimate cited in 1995 by the chief prosecutor of Florence suggested that organised criminal groups in Russia then **controlled** 35 per cent of the commercial banks, 40 per cent of former State-owned industry, 35 per cent of private enterprise — and as much as 60 per cent of commerce and 80 per cent of joint ventures with foreign firms.	Commercial banks, former state-owned industry, private enterprise, commerce, joint ventures with foreign firms
p.120–121	To reduce or even limit the economic wealth and potential for political and social disruption of these transnational criminal groups to manageable levels would strike at the very heart of national sovereignty [...] If then suppression as an option is blocked by the refusal of state governments to give up their **control** of law enforcement, an alternative option would be to decriminalise the drug trade.	Law enforcement
p.130	By the early 1990s, it had run into balance of payments problems and needed the blessing and support of the IMF — where, again, the US exercised the **controlling** veto power.	Veto power

Page	Quote	Object
p.138	But why, the political economist will ask, did states allow such great **authority** and influence to be exercised within the limits of the law by such a small number of private firms? One answer lies in the preference of governments in the Anglo-Saxon tradition for indirect rule, leaving it, wherever possible, to the operators themselves to monitor and **control** themselves, whether they are doctors, lawyers, stockbrokers or insurers.	Indirect rule within the law
p.147	There is also an element of private protectionism when a firm has monopoly **control** over a technology, or a system of marketing, or a brand-name that keeps away competitors.	Technology
p.149	Yet she admits that the most effective cartel of the four she studied, that in diamonds, almost entirely owed its success to the tight **control** over supplies exercised by one firm, Anglo-American, and the majority owners, the Oppenheimer family.	Supplies
p.179	Transfer of **authority** from the member governments to federal institutions over this central responsibility of political **authority** in a market economy has not yet happened. Nor has the replacement of national defence forces by a European Army under **control** of a European Chief of Staff. [...] It seems that European governments — though they are reluctant to say so — really prefer a vacuum of power over key matters of security, currency, law and order and foreign policy to a real transfer of power to supranational institutions.	National defence forces
p.187	Other states which formerly had **controlled** and managed their national markets now found their PTTs challenged by the combination of new technology and foreign competitors. State policies changed in response.	National markets

Page	Quote	Object
p.193	There is no world central bank to exercise the judicious **control** over the creation of credit and the expansion of the money supply that historical experience has shown needs to be exercised. There is no world central bank with powers to **control** and regulate a banking system that operates transnationally in internationally integrated financial markets.	Banking system that operates transnationally in internationally integrated financial markets
p.197	The concentration of power in what Perry Anderson called the absolutist state was the means by which a politically **controlled** framework of rules was put round the emerging capitalist or market economy.	Political framework of rules

Source: STRANGE, 1996.

Appendix 5 – Articles Published in 2013

Table 5 – No. of Articles Published by Subject in 2013

Subject	**N**
Tor Project	13
Silk Road	12
Edward Snowden	6
Eric Eoin Marques	2
Pirate Bay	2
Freedom Hosting	1
Sheep Marketplace	1
Chelsea Manning	1
"Deep Web" (Multiple Actors)	1
WikiLeaks	1
Strongbox	1
Total	**41**

Source: Author.

Appendix 6 – Articles Published in 2014

Table 6 – No. of Articles Published by Subject in 2014

Subject	**N**
Tor Project	16
Silk Road 2.0	12
Pornography	6
Privacy	5
Silk Road	4
Edward Snowden	3
Silk Road 3.0	2
Facebook	2
Books on DarkNet	2
Humanity	1
BitCoin	1
Digital Activism	1
Surveillance	1
SimpleLocker Android Malware	1
Onion Ransomware	1
Doxbin	1
X-Net Group	1
WikiLeaks	1
Total	**61**

Source: Author.

Appendix 7 – Articles Published in 2017

Table 7 – No. of Articles Published by Subject in 2017

Actor	**N**
Alphabay	9
Pornography	5
Hacker Arrest	2
Tor Project	2
Cyber Attack	1
Privacy	1
Malwares	1
Ransomware	1
Google Incognito Mode	1
Drug Overdose	1
Russia Internet Censor	1
Total	**25**

Source: Author.

Appendix 8 – Articles and Occurrences for Analysis by Year

Table 8 – No. of Articles Analyzed and No. of Total Occurrences for Analysis (2007–2017)

Year	A	O	R
2007	1	1	0
2008	2	2	0
2009	2	2	0
2010	1	2	1
2011	2	2	0
2012	2	2	0
2013	34	39	5
2014	42	49	7
2015	19	20	1
2016	8	8	0
2017	12	12	0
Total	**125**	**139**	**14**

*Analyzed (A); Occurrences (O); Repeated (R)

Source: Author.

Appendix 9 – Diffusion Analysis by Actor and Group

Table 9 – Groups and Actors: Number of Occurrences (N) by Dimension through Journalistic Publications (2007–2017)

			Authority			Control			Outcomes	
Group	**Actor**	**Occ.**	**Decr.**	**Stab.**	**Grow.**	**None**	**Part.**	**Abs.**	**Non-alt.**	**Alt.**
Surveillance Circumvention		**53**	**9**	**18**	**26**	**0**	**3**	**50**	**36**	**17**
	Tor Project	50	9	16	25	0	0	50	33	17
	Facebook	3	0	2	1	0	3	0	3	0
Digital Security		**7**	**1**	**0**	**6**	**1**	**3**	**3**	**2**	**5**
	Carnegie Mellon University	1	0	0	1	0	1	0	0	1
	Dan Egerstad	1	0	0	1	1	0	0	0	1
	Freedom Hosting	1	1	0	0	0	0	1	1	0
	Iranian Cyber Army	1	0	0	1	0	1	0	1	0
	Onion Ransomware	1	0	0	1	0	1	0	0	1
	Ransomware	1	0	0	1	0	0	1	0	1
	SimpleLocker Android Malware	1	0	0	1	0	0	1	0	1
Journalism & Whistleblowing		**21**	**0**	**5**	**16**	**1**	**19**	**1**	**8**	**13**
	Edward Snowden	11	0	2	9	0	11	0	3	8
	WikiLeaks	3	0	1	2	1	2	0	0	3
	SecureDrop System	2	0	0	2	0	2	0	2	0
	ProPublica	1	0	0	1	0	0	1	1	0
	Harold T. Martin	1	0	1	0	0	1	0	1	0
	Strongbox	1	0	0	1	0	1	0	1	0
	Chelsea Manning	1	0	1	0	0	1	0	0	1
	X-Net Group	1	0	0	1	0	1	0	0	1
Online Marketplace		**57**	**47**	**5**	**5**	**0**	**29**	**28**	**15**	**42**
	Silk Road	28	21	4	3	0	1	27	5	23
	Silk Road 2.0	14	14	0	0	0	14	0	6	8
	Alphabay	9	9	0	0	0	9	0	0	9
	Silk Road 3.0	2	0	0	2	0	2	0	2	0
	Farmer's Market	2	2	0	0	0	2	0	0	2
	Evolution	1	0	1	0	0	1	0	1	0

Continued on next page

			Authority			Control			Outcomes	
Group	**Actor**	**Occ.**	**Decr.**	**Stab.**	**Grow.**	**None**	**Part.**	**Abs.**	**Non-alt.**	**Alt.**
	Sheep Marketplace	1	1	0	0	0	0	1	1	0
Privacy		**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**
	Doxbin	1	0	1	0	0	1	0	1	0
Total		**139**	**57**	**29**	**53**	**2**	**55**	**82**	**62**	**77**

Source: Author.

Appendix 10 – Article Database for Analysis

Table 10 – Article Database: Journalistic Articles and Coded Occurrences for Diffusion of Power Analysis (2007–2017)

#	Country	Newspaper	Article Title	Author	Year	Actor	Category	Peers	Auth.	Object	Ctrl.	Status Quo	Outc.	Effect on Reality	Rep. Art.
1	USA	The Washington Post	"Researcher intercepted embassy passwords"	Jeremy Kirk	September 2007	Dan Egerstad	Digital Security	Embassies, technical experts	1	Tor Network	0	No one knew the embassies' logins and passwords and could not use them	1	YES	NO
2	UK	The Guardian	"Vaulting the great firewall"	Dmitri Vitaliev	August 2008	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	Censorship	1	YES	NO
3	UK	The Guardian	"Chaos aims to crack China's wall"	Danny Bradbury	August 2008	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	Censorship	1	YES	NO
4	USA	The Washington Post	"The Anatomy of The Twitter Attack: Part II"	Nik Cubrilovic	December 2009	Iranian Cyber Army	Digital Security	Hackers, Twitter Users, technical experts	1	DNS Records at company "Dyn" (redirected to the Tor Network)	1	Intact Logins and Passwords	0	NO	NO
5	UK	The Guardian	"Using proxies to get around censors"	Kevin Anderson	July 2009	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	Censorship	1	YES	NO
6	USA	The NY Times	"Granting Anonymity"	Virginia Heffernan	December 2010	Wikileaks	Journalism & Whistleblowing	Governments, journalists, worldwide citizens, activists	1	Storage of information	0	Government Privacy	1	YES	NO
7	USA	The NY Times	"Granting Anonymity"	Virginia Heffernan	December 2010	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	Not being able to choose what you keep private on the Internet (virtual)	0	NO	NO
8	UK	The Telegraph	"Amazon cloud boosts Tor dissident network"	Telegraph	November 2011	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	No donation of bandwidth on the Tor Network (relay)	0	NO	NO

Continued on next page

Table – continued from previous page

#	Country	Newspaper	Article Title	Author	Year	Actor	Category	Peers	Auth.	Object	Ctrl.	Status Quo	Outc.	Effect on Reality	Rep. Art.
9	UK	The Telegraph	"Iran cracks down on web dissident technology"	Christopher Williams	March 2011	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	−1	Tor Network	2	The ongoing operation of the Tor Network	1	YES	NO
10	USA	MLIVE.com	"Coldwater man among 15 arrests in international online narcotics drug probe"	The Associated Press	April 2012	Farmer's Market	Online Marketplace	Private citizens	−1	Marketplace Site	1	No trade of illegal products	1	YES	NO
11	USA	NJ.com	"Several arrests made in international online narcotics scheme, including N.J. resident"	The Associated Press	April 2012	Farmer's Market	Online Marketplace	Private citizens	−1	Marketplace Site	1	No trade of illegal products	1	YES	NO
12	USA	The Washington Post	"A bunch of Tor sites spread malware. Was the FBI behind it?"	Andrea Peterson	August 2013	Freedom Hosting	Digital Security	Private citizens	−1	Server	2	Law and order	0	NO	NO
13	UK	The Guardian	"Attacking Tor: how the NSA targets users' online anonymity"	Bruce Schneier	October 2013	Edward Snowden	Journalism & Whistleblowing	Governments, private citizens, journalists, activists, dissidents	1	Information on NSA surveillance, including on Tor Network (with documents)	1	Organizations, private citizens and activists not reacting to the NSA	0	NO	NO
14	USA	AL.com	"Auburn institute the clue that led to Silk Road online drug marketplace bust"	Mia Watkins	October 2013	Silk Road	Online Marketplace	Private citizens	−1	Marketplace Site and its mechanisms to function	2	Law and order: to not purchase illegal products	1	YES	NO
15	USA	The NY Times	"Cyber Subterfuge"	Misha Glenny	November 2013	Edward Snowden	Journalism & Whistleblowing	Governments, private citizens, journalists, activists, dissidents	1	Information on NSA surveillance, including on Tor Network (with documents)	1	Organizations, private citizens and activists not reacting to the NSA	1	YES	NO
16	USA	The Washington Post	"Everything you need to know about the NSA and Tor in one FAQ"	Timothy B. Lee	October 2013	Edward Snowden	Journalism & Whistleblowing	Governments, private citizens, journalists, activists, dissidents	1	Information on NSA surveillance, including on Tor Network (with documents)	1	No debates and articles on the mass surveillance scheme	1	YES	NO
17	UK	The Guardian	"FBI claims largest Bitcoin seizure after arrest of alleged Silk Road founder"	James Ball, Charles Arthur and Adam Gabatt	October 2013	Silk Road	Online Marketplace	Private citizens	−1	Marketplace Site and its payment mechanism	2	Law and order: to not purchase illegal products	1	YES	NO
18	UK	The Telegraph	"Filesharing search engines take to dark web and Bitcoin to escape Hollywood"	Samuel Gibbs	November 2013	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	Steady number of users	0	NO	NO
19	USA	The Washington Post	"Five ways to stop the NSA from spying on you"	Timothy B. Lee	June 2013	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	Steady number of users	0	NO	NO

Continued on next page

Table – continued from previous page

#	Country	Newspaper	Article Title	Author	Year	Actor	Category	Peers	Auth.	Object	Ctrl.	Status Quo	Outc.	Effect on Reality	Rep. Art.
20	UK	The Guardian	"How a Russian cybercriminal tried to frame me with a Bitcoin heroin deal"	Brian Krebs	July 2013	Silk Road	Online Marketplace	Private citizens	1	Marketplace Site and its payment mechanism	2	Law and order: to not purchase illegal products	1	YES	NO
21	UK	Daily Mail	"How top drug dealer on dark net Silk Road was working with FBI informant for months before huge bust"	Daily Mail Reporter	October 2013	Silk Road	Online Marketplace	Private citizens	−1	Marketplace Site and its payment mechanism	2	Law and order: to not purchase illegal products	1	YES	NO
22	UK	The Guardian	"Anonymous marketplace that replaced Silk Road VANISHES... Taking $100M of users' money with it"	Joshua Gardner	December 2013	Sheep Marketplace	Online Marketplace	Private citizens	−1	Marketplace Site and its payment mechanism	2	Law and order: to not purchase illegal products	0	NO	NO
23	UK	The Guardian	"Internet security: 10 ways to keep your personal data safe from online snoopers"	John Naughton	September 2013	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	To not keep personal data safe from online snoopers	0	NO	NO
24	USA	The Washington Post	"It's a mystery: Why is Tor usage doubling all of a sudden?"	Brian Fung	August 2013	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	Steady number of users	0	NO	NO
25	UK	Daily Mail	"It's not just child porn: Fake passports, guns, cocaine, even hitmen for hire are a few clicks away on the internet"	Steve Boggan	November 2013	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	No effects in real life	1	YES	YES
26	UK	Daily Mail	"It's not just child porn: Fake passports, guns, ecocaine, even hitmen for hire are a few clicks away on the internet"	Steve Boggan	November 2013	Silk Road	Online Marketplace	Private citizens	−1	Marketplace Site and its payment mechanism	2	Law and order: to not purchase illegal products	1	YES	NO
27	UK	The Telegraph	"National Crime Agency wages war on Tor 'darknet' anonymity"	Sophie Curtis	October 2013	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	No effects in real life	1	YES	NO
28	UK	The Telegraph	"New Silk Road drugs website open"	Reuters (edited by Bonnie Malkin)	November 2013	Silk Road	Online Marketplace	Private citizens	0	Marketplace Site and its payment mechanism	2	Law and order: to not purchase illegal products	0	NO	NO
29	UK	The Guardian	"NSA and GCHQ target Tor network that protects anonymity of web users"	James Ball, Bruce Schneier and Glenn Greenwald	October 2013	Edward Snowden	Journalism & Whistleblowing	Governments, private citizens, journalists, activists, dissidents	1	Information on NSA surveillance, including on Tor Network (with documents)	1	No actions specifically targeting NSA	0	NO	NO

Continued on next page

Table – continued from previous page

#	Country	Newspaper	Article Title	Author	Year	Actor	Category	Peers	Auth.	Object	Ctrl.	Status Quo	Outc.	Effect on Reality	Rep. Art.
30	UK	The Guardian	"NSA Files: Decoded – Caught in a 'Net"'	Nadja Popovich and Greg Chen	November 2013	Edward Snowden	Journalism & Whistleblowing	Governments, private citizens, journalists, activists, dissidents	1	Information on NSA surveillance, including on Tor Network (with documents)	1	Governments and citizens stunned and not taking action	1	YES	NO
31	UK	The Guardian	"NSA Files: Decoded – Pretty Good Privacy"	Greg Chen and Gabriel Dance	November 2013	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	No actions toward anonymity and privacy	0	NO	NO
32	USA	The Washington Post	"NSA report on the Tor encrypted network"	The Washington Post	January 2014	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	No effects in real life	0	NO	NO
33	UK	Daily Mail	"Pictured: The Utah grandfather who lived a double life as a drug dealer working for the online black market Silk Road... before its founder tried to have him killed for $80,000 "	Daily Mail Reporter	November 2013	Silk Road	Online Marketplace	Private citizens	−1	Marketplace Site and its payment mechanism	2	Law and order: to not purchase illegal products	1	YES	NO
34	UK	The Guardian	"Privacy and surveillance: Jacob Applebaum, Caspar Bowden and more"	Charles Arthur	September 2013	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	No action by the NSA	1	YES	NO
35	UK	Daily Mail	"Man accused of operating notorious online drug market Silk Road (and earning $80 million in commission) ordered to New York to face charges"	The Associated Press	October 2013	Silk Road	Online Marketplace	Private citizens	−1	Marketplace Site and its payment mechanism	2	Law and order: to not purchase illegal products	1	YES	NO
36	USA	The Washington Post	"Secret NSA documents show campaign against Tor encrypted network"	Barton Gellman, Craig Timberg and Steven Rich	October 2013	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	No actions by the NSA	0	NO	YES
37	USA	The Washington Post	"Secret NSA campaign against Tor encrypted network"	Barton Gellman, Craig Timberg and Steven Rich	October 2013	Edward Snowden	Journalism & Whistleblowing	Governments, private citizens, journalists, activists, dissidents	1	Information on NSA surveillance, including on Tor Network (with documents)	1	No discussion on NSA and mass surveillance schemes	1	YES	NO
38	UK	The Guardian	"Silk Road could have led the way to safer drug use"	Oscar Rickett	October 2013	Silk Road	Online Marketplace	Private citizens	−1	Marketplace and its payment mechanism	2	–	0	NO	NO

Continued on next page

Table – continued from previous page

#	Country	Newspaper	Article Title	Author	Year	Actor	Category	Peers	Auth.	Object	Ctrl.	Status Quo	Outc.	Effect on Reality	Rep. Art.
39	UK	Daily Mail	"Man behind Silk Road drug gang 'planned to carry out six murders"'	Shari Miller	November 2013	Silk Road	Online Marketplace	Private citizens	−1	Marketplace Site	2	Law and order: to not purchase illegal products	1	YES	NO
40	UK	The Guardian	"Silk Road underground market closed but others will replace it"	Samuel Gibbs	October 2013	Silk Road	Online Marketplace	Private citizens	0	Marketplace Site and its mechanism	2	–	0	NO	YES
41	UK	The Guardian	"Silk Road underground market closed but others will replace it"	Samuel Gibbs	October 2013	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	Law and order: no trade of illicit drugs on the Internet	0	NO	NO
42	UK	The Guardian	"Silk Road website did roaring trade in Tesco Clubcard vouchers"	Jamie Doward	March 2014	Silk Road	Online Marketplace	Private citizens	0	Marketplace Site and its payment mechanism	2	Law and order: to not purchase illegal products	1	YES	NO
43	UK	The Guardian	"Strongbox: New Yorker's safe in the 'war between data capture and privacy"'	Ed Pilkington	May 2013	Wikileaks	Journalism & Whistleblowing	Private citizens, dissidents, journalists, activists, state governments	0	Storage of information and its storage (software)	1	No discussion on NSA, US government actions, worldwide state governments	1	YES	YES
44	UK	The Guardian	"Strongbox: New Yorker's safe in the 'war between data capture and privacy"'	Ed Pilkington	May 2013	Strongbox	Journalism & Whistleblowing	Private citizens, dissidents, journalists, activists, state governments	1	Channel of communication and its storage (software)	1	No leakage, no information sharing on Tor documents	0	NO	YES
45	UK	The Guardian	"Strongbox: New Yorker's safe in the 'war between data capture and privacy"'	Ed Pilkington	May 2013	Chelsea Manning	Journalism & Whistleblowing	Private citizens, dissidents, journalists, activists, state governments	0	Documents from the NSA	1	No leakage, incarceration, publication of secret documents	1	YES	NO
46	USA	The Washington Post	"Talk by Roger Dingledine of Torproject.org at the NSA"	Washington Post Staff	October 2013	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	–	0	NO	NO
47	UK	The Guardian	"Tech 128: PewDiePie, PS4, selfies and self-driving cars"	Samuel Gibbs, Alex Hern, Charles Arthur, Siraj Datoo and Kirsty Beckingham	December 2013	Silk Road	Online Marketplace	Private citizens	0	Marketplace Site and its payment mechanism	2	–	0	NO	NO
48	UK	The Guardian	"Tech 128: Silk Road, Spotify and Tinder"	Samuel Gibbs, Alex Hern, Charles Arthur, Siraj Datoo and Kirsty Beckingham	December 2013	Silk Road	Online Marketplace	Private citizens	−1	Marketplace Site and its payment mechanism	2	–	0	NO	NO

Continued on next page

Table – continued from previous page

#	Country	Newspaper	Article Title	Author	Year	Actor	Category	Peers	Auth.	Object	Ctrl.	Status Quo	Outc.	Effect on Reality	Rep. Art.
49	USA	The Washington Post	"The feds pay for 60 percent of Tor's development. Can users trust it?"	Brian Fung	September 2013	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	–	0	NO	NO
50	UK	The Guardian	"Tor: 'The king of high-secure, low-latency anonymity"'	The Guardian	October 2013	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	–	0	NO	NO
51	UK	The Telegraph	"Users of darknet websites advised to dump Windows"	Sophie Curtis	August 2013	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	–	0	NO	NO
52	UK	The Guardian	"What is Tor? A beginner's guide to the privacy tool"	Stuart Dredge	November 2013	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	Parliament not discussing cybertools and privacy	1	YES	NO
53	USA	NOLA.com	"17 arrested in worldwide drug website bust; Silk Road 2.0 shut down"	The Associated Press	November 2014	Silk Road 2.0	Online Marketplace	Private citizens	−1	Marketplace Site	1	–	0	NO	NO
54	USA	The Washington Post	"A Q&A with the hackers who say they helped break into Sony's network"	Brian Fung	December 2014	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	−1	Tor Network	2	–	0	NO	NO
55	USA	Oregon Live.com	"Dark net investigation cracks down on Silk Road 2.0; 17 arrested"	The Associated Press	November 2014	Silk Road 2.0	Online Marketplace	Private citizens	−1	Marketplace Site	1	–	0	NO	NO
56	UK	Daily Mail	"Dark Web drug site challenge law enforcement"	The Associated Press	November 2014	Silk Road 3.0	Online Marketplace	Private citizens	1	Marketplace Site	1	–	0	NO	NO
57	USA	NOLA.com	"Dark Web illegal drug exchanges challenge law enforcement"	The Associated Press	November 2014	Silk Road 3.0	Online Marketplace	Private citizens	1	Marketplace Site	1	–	0	NO	NO
58	USA	The Washington Post	"Does obtaining leaked data from a misconfigured website violate the CFAA?"	Orin Kerr	September 2014	Silk Road	Online Marketplace	Private citizens	−1	Marketplace Site and its payment mechanism	1	No implications for the Computer Fraud and Abuse Act (the federal computer hacking statute, USA)	1	YES	NO
59	UK	Daily Mail	"Europol: 17 arrests in worldwide drug website bust"	The Associated Press	November 2014	Silk Road 2.0	Online Marketplace	Private citizens	−1	Marketplace Site	1	–	0	YES	YES

Continued on next page

Table – continued from previous page

#	Country	Newspaper	Article Title	Author	Year	Actor	Category	Peers	Auth.	Object	Ctrl.	Status Quo	Outc.	Effect on Reality	Rep. Art.
60	UK	Daily Mail	"Europol: 17 arrests in worldwide drug website bust"	The Associated Press	November 2014	Silk Road 2.0	Online Marketplace	Private citizens	−1	Marketplace Site	1	–	0	YES	NO
61	UK	The Guardian	"Evidence implicates government backeed hackers in Tor malware attacks"	Tom Fox-Brewster	November 2014	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	–	0	NO	NO
62	UK	The Guardian	"Facebook opens up to anonymous Tor users with .onion address"	Tom Fox-Brewster	October 2014	Facebook	Surveillance Circumvention	Private citizens	0	Facebook Website through Tor Network	1	–	0	NO	NO
63	USA	The Washington Post	"FBI arrests man for allegedly creating 'Silk Road 2.0' to sell drugs on the 'Dark Web"'	Craig Timberg	November 2014	Silk Road 2.0	Online Marketplace	Private citizens	−1	Marketplace Site	1	No trade of illegal products	1	YES	NO
64	USA	The NY Times	"German Student Under N.S.A. Scrutiny, Reports Say"	Alison Smale	July 2014	Edward Snowden	Journalism & Whistleblowing	Governments, private citizens, journalists, activists, dissidents	1	Information on NSA surveillance, including on Tor Network (with documents)	1	No lawmakers beginning a formal inquiry in Germany	1	YES	NO
65	UK	The Guardian	"Global Drug Survey findings: more people buying drugs online in the UK"	Ami Sedghi	April 2014	Silk Road	Online Marketplace	Private citizens	1	Marketplace Site and its payment mechanism	2	Steady number of people consuming drugs through online purchases	1	YES	NO
66	UK	The Guardian	"Guardian launches SecureDrop system for whistleblowers to share files"	James Ball	June 2014	SecureDrop System	Journalism & Whistleblowing	Private citizens, journalists, state governments	1	Channel of communication and its storage (software)	1	Newspaper, journalists on the Tor Network for documents	0	NO	YES
67	UK	The Guardian	"Guardian launches SecureDrop system for whistleblowers to share files"	James Ball	June 2014	Edward Snowden	Journalism & Whistleblowing	Governments, private citizens, journalists, activists, dissidents	1	Information on NSA surveillance, including on Tor Network (with documents)	1	Newspaper not reacting to the leaks	1	YES	NO
68	USA	The NY Times	"International Raids Target Sites Selling Contraband on the 'Dark Web"'	Benjamin Weiser and Doreen Carvajal	November 2014	Silk Road 2.0	Online Marketplace	Private citizens	−1	Marketplace Site	1	No trade of illegal products	1		YES
69	UK	The Guardian	"Life after Silk Road: how the darknet drugs market is booming"	Mike Power	May 2014	Silk Road	Online Marketplace	Private citizens	1	Marketplace Site and its payment mechanism	2	Buying drugs online is a niche activity	1	YES	NO
70	UK	The Guardian	"New ransomware employs Tor to stay hidden from security"	Alex Hern	July 2014	Onion Ransomware	Digital Security	Private citizens, digital activists, state government	1	Channel of communication and its storage (software)	1	No payments	1	YES	NO
71	UK	The Guardian	"Operation Onymous: may have exposed flaws in Tor, developers reveal"	Alex Hern	November 2014	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	−1	Tor Network	2	No collaboration of authorities to track criminals on Tor Network	1	YES	YES
72	UK	The Guardian	"Operation Onymous: may have exposed flaws in Tor, developers reveal"	Alex Hern	November 2014	Silk Road 2.0	Online Marketplace	Private citizens	−1	Marketplace	1	–	0	NO	NO

Continued on next page

Table – continued from previous page

#	Country	Newspaper	Article Title	Author	Year	Actor	Category	Peers	Auth.	Object	Ctrl.	Status Quo	Outc.	Effect on Reality	Rep. Art.
73	UK	The Guardian	"Researchers: Lawyers blocked our Black hat demo on the anonymising Tor"	Tom Brewster	July 2014	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	−1	Tor Network	2	–	0	NO	NO
74	UK	The Guardian	"Russia offers 3.9m rubles for 'research' to identify users of Tor"	Alec Luhn	July 2014	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	–	0	NO	NO
75	UK	Daily Mail	"Silk Road 2.0 shut down, alleged US operator charged"	AFP	November 2014	Silk Road 2.0	Online Marketplace	Private citizens	−1	Marketplace Site	1	No trade of illegal products	1	YES	NO
76	UK	The Telegraph	"Silk Road 2.0 targeted in Operation Onymous' darkweb takedown"	Tom Fox-Brewster	November 2014	Silk Road 2.0	Online Marketplace	Private citizens	−1	Marketplace Site	1	No trade of illegal products	1	YES	NO
77	USA	The Washington Post	"Silk Road 2.0 Web site leads to arrest, charges"	Craig Timberg	November 2014	Silk Road 2.0	Online Marketplace	Private citizens	−1	Marketplace Site	1	No trade of illegal products	1	YES	NO
78	UK	The Guardian	"Silk Road 2.0's alleged owner arrested as drugs website shuttered by FBI"	Dominic Rushe	November 2014	Silk Road 2.0	Online Marketplace	Private citizens	−1	Marketplace Site	1	No trade of illegal products	1	YES	NO
79	UK	Daily Mail	"Silk Road 2.0's alleged owner arrested as drugs website shuttered by FBI"	Daily Mail	November 2014	Silk Road 2.0	Online Marketplace	Private citizens	−1	Marketplace Site	1	No trade of illegal products	1	YES	NO
80	UK	Daily Mail	"Silicon Valley software engineer, 26, arrested for setting up Silk Road style drug dealing site: FBI take former Space X employee into custody in San Francisco raid"	The Associated Press and Mark Prigg	November 2014	Silk Road 2.0	Online Marketplace	Private citizens	−1	Marketplace Site	1	No trade of illegal products	1	YES	NO
81	UK	The Guardian	"Simplelocker Android Malware locks up mobile data and demands a ransom"	Tom Brewster	June 2014	SimpleLocker Android Malware	Digital Security	Private citizens	1	Channel of communication and its storage (software)	2	No kidnapping of digital files and rescue money	1	YES	NO
82	UK	Daily Mail	"Spain's 'X-net' corruption fighters expose graft"	The Associated Press	December 2014	X-Net Group	Journalism & Whistleblowing	Private citizens	1	Channel of communication and its storage (software)	1	Not using the mechanism to fight corruption and file lawsuits in the Spanish courts	1	YES	YES
83	UK	Daily Mail	"Spain's 'X-net' corruption fighters expose graft"	The Associated Press	December 2014	Wikileaks	Journalism & Whistleblowing	Governments, journalists, worldwide citizens, activists	1	Channel of communication and its storage (software)	1	Not inspiring social movements in local communities	1	YES	YES
84	UK	Daily Mail	"Spain's 'X-net' corruption fighters expose graft"	The Associated Press	December 2014	Edward Snowden	Journalism & Whistleblowing	Governments, private citizens, journalists, activists, dissidents	1	Information on NSA surveillance, including on Tor Network (with documents)	1	–	0	NO	NO

Continued on next page

Table – continued from previous page

#	Country	Newspaper	Article Title	Author	Year	Actor	Category	Peers	Auth.	Object	Ctrl.	Status Quo	Outc.	Effect on Reality	Rep. Art.
85	UK	The Guardian	"The darkweb's nihilistic vigilante sees the light"	Tom Fox-Brewster	December 2014	Doxbin	Privacy	Private citizens	0	Central Site for Publication of private informations and others	1	–	0	NO	NO
86	USA	The Washington Post	"The hackers who say they took down gaming networks are now going after Tor"	Andrea Peterson and Brian Fung	December 2014	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	–	0	NO	NO
87	UK	Daily Mail	"The internet is becoming a 'dark and ungoverned' place where paedophiles, murderers and terrorists can safely operate, warns Met chief"	Gemma Mullin	November 2014	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	–	0	NO	NO
88	UK	The Telegraph	"Tor admits hackers have unmasked 'anonymous' users"	Matthew Sparkes	July 2014	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	−1	Tor Network	2	–	0	NO	NO
89	USA	A.com	"The Switchboard: 'Spoiler Onions' on the Tor network"	Andrea Peterson	January 2014	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	−1	Tor Network	2	–	0	NO	NO
90	UK	The Guardian	"Tor users advised to check their computers for malware"	Alex Hern	October 2014	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	−1	Tor Network	2	–	0	NO	NO
91	UK	The Guardian	"Tor attack may have revealed user identities, project warns"	Samuel Gibbs	July 2014	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	No public speeches on Tor Network	1	YES	NO
92	UK	The Guardian	"Tor may be forced to cut bot capacity after Heartbleed bug"	Alex Hern	April 2014	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	–	0	NO	NO

Continued on next page

#	Country	Newspaper	Article Title	Author	Year	Actor	Category	Peers	Auth.	Object	Ctrl.	Status Quo	Outc.	Effect on Reality	Rep. Art.
93	USA	The Washington Post	"Why was the Black Hat talk on Tor deanonymization mysteriously canceled?"	Andrea Peterson	July 2014	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	No public speeches on Tor Network	1	YES	NO
94	USA	The Washington Post	"U.S., European authorities strike against Internet's black markets"	Craig Timberg and Nakashima	November 2014	Silk Road 2.0	Online Marketplace	Private citizens	−1	Marketplace	1	–	0	NO	YES
95	USA	The Washington Post	"U.S., European authorities strike against Internet's black markets"	Craig Timberg and Edward Nakashima	November 2014	Edward Snowden	Journalism & Whistleblowing	Governments, private citizens, journalists, activists, dissidents	0	Information on NSA surveillance, including on Tor Network (with documents)	1	NSA not concentrating on Tor Network	1	YES	YES
96	USA	The Washington Post	"U.S., European authorities strike against Internet's black markets"	Craig Timberg and Nakashima R	November 2014	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	−1	Tor Network	2	–	0	NO	NO
97	UK	The Guardian	"US government increases funding for Tor, giving $1.8m in 2013"	Alex Hern	July 2014	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	No funding from the US government	1	YES	NO
98	UK	Daily Mail	"Is this the most secure smartphone in the world? BOSS Phone is the first to use an Onion Router to allow anonymous browsing"	Richard Gray	January 2015	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	Cellphones blocked in authoritarian countries	1	YES	NO
99	USA	The Washington Post	"With Tor, Facebook is first social media giant to venture into the 'dark Web"'	Justin Moyer	November 2014	Facebook	Surveillance Circumvention	Private citizens	0	Facebook Website through Tor Network	1	–	0	NO	NO
100	USA	NJ.com	"Drier: Is Comcast really blocking anonymous Internet Browser Tor?"	Troy Dreier	September 2014	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	–	0	NO	NO
101	USA	The NY Times	"At Silk Road Trial, Lawyers Fight to include Evidence They Call Vital: Emoji"	Benjamin Weiser	January 2015	Silk Road	Online Marketplace	Private citizens	−1	Marketplace and its payment mechanism	2	No courtroom decisions and judgments of private citizens over use of Tor or online marketplaces	1	YES	NO

Continued on next page

#	Country	Newspaper	Article Title	Author	Year	Actor	Category	Peers	Auth.	Object	Ctrl.	Status Quo	Outc.	Effect on Reality	Rep. Art.
102	USA	Penn Live.com	"From Penn State student to Dread Pirate Roberts: Tale of the Silk Road drug kingpin"	Nick Malawskey	February 2015	Silk Road	Online Marketplace	Private citizens	−1	Marketplace and its payment mechanism	2	No courtroom decisions and judgments of private citizens over use of Tor or marketplace	1	YES	NO
103	USA	The Washington Post	"Facebook claims spike in government data requests; online review bill to get committee vote; did the FBI hack Tor?"	Elise Viebeck	November 2015	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	−1	Tor Network	2	–	0	NO	NO
104	UK	The Telegraph	"How to stop your boss spying on you at work"	Sophie Curtis	October 2015	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	Boss spy on worker's communications	1	YES	NO
105	USA	The Washington Post	"In Russia, political engagement is blossoming online"	Andrei Soldatov and Irina Borogan	December 2015	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	Kremlin not hesitant to outlaw the Tor Network	1	YES	NO
106	UK	The Guardian	"Is Ross Ulbricht, Silk Road's pirate king a mobster or a martyr?"'	Jamie Doward	May 2015	Silk Road	Online Marketplace	Private citizens	−1	Marketplace Site and its payment mechanism	2	No deaths of private citizens	1	YES	NO
107	UK	Daily Mail	"Gang of university business students who modelled themselves on Breaking Bad ran drugs empire that sold ectasy, cannabis and LSD to students on hidden 'Dark Web' "	Euan McLelland	August 2015	Silk Road	Online Marketplace	Private citizens	−1	Marketplace Site and its mechanism	2	No drug sellers benefiting from Online Marketplaces (having it easier)	1	YES	NO
108	INDIA	The Tribune	"Private data, public life"	Anurag Chakraborty	July 2015	Edward Snowden	Journalism & Whistleblowing	Governments, private citizens, journalists, activists, dissidents	0	Information on NSA surveillance, including on Tor Network (with documents)	1	No reactions from the globe	1	YES	YES
109	INDIA	The Tribune	"Private data, public life"	Anurag Chakraborty	July 2015	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	–	0	NO	NO
110	UK	Daily Mail	"Mastermind behind $180M 'eBay of drugs' Silk Road convicted after jury deliberates just three hours"	AP	February 2015	Silk Road	Online Marketplace	Private citizens	−1	Marketplace Site and its payment mechanism	2	No drug sellers benefiting from Online Marketplaces (having it easier)	1	YES	NO
111	UK	The Telegraph	"Silk Road founder: 'It ruined my life and destroyed my future"'	Rhiannon Williams and agency	May 2015	Silk Road	Online Marketplace	Private citizens	−1	Marketplace Site and its mechanism	2	No huge drug sales on online marketplaces	1	YES	NO

Continued on next page

Table – continued from previous page

#	Country	Newspaper	Article Title	Author	Year	Actor	Category	Peers	Auth.	Object	Ctrl.	Status Quo	Outc.	Effect on Reality	Rep. Art.
112	UK	The Guardian	"Silk Road founder: 'It ruined my life and destroyed my future"'	Nicky Woolf	January 2015	Silk Road	Online Marketplace	Private citizens	−1	Marketplace Site and its mechanism	2	No drugs being traded over an online marketplace	1	YES	NO
113	UK	Daily Mail	"Silk Road mastermind Ross Ulbricht sentenced to life in jail for creating worldwide criminal enterprise that sold more than $200 million worth of drugs"	Reuters and Associated Press	May 2015	Silk Road	Online Marketplace	Private citizens	−1	Marketplace Site and its mechanism	2	No drugs being traded over an online marketplace	1	YES	NO
114	UK	The Guardian	"Surveillance Q&A: what web data is affected and how to fool the snoopers"	Samuel Gibbs	November 2015	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	–	0	NO	NO
115	USA	The NY Times	"Trial Over a Man's Role in a Black Market Begins"	Benjamin Weiser	January 2015	Silk Road	Online Marketplace	Private citizens	−1	Marketplace Site and its payment mechanism	2	No drugs being traded over an online marketplace	1	YES	NO
116	UK	Daily Mail	"US marshals to auction 50,000 bitcoins worth $11 million that were confiscated from convicted Silk Road mastermind"	Reuters	February 2015	Silk Road	Online Marketplace	Private citizens	−1	Marketplace and its payment mechanism	2	No drugs being traded over an online marketplace	1	YES	NO
117	UK	Daily Mail	"US Marshals to auction dark web drug dealer's $11 million bitcoin fortune: Bidders get the chance to buy Silk Road founder Ross Ulbricht's fortine... at a discount"	Darren Boyle	October 2015	Silk Road	Online Marketplace	Private citizens	−1	Marketplace and its payment mechanism	2	No drug being traded over an online marketplace	1	YES	NO
118	USA	The Washington Post	"Why 'Dark Web' drug markets will keep on imploding"	Henry Farrell	March 2015	Evolution	Online Marketplace	Private citizens	0	Marketplace Site	1	–	0	NO	NO
119	UK	Daily Mail	"Browse free or die? New Hampshire library is at privacy fore"	The Associated Press	June 2015	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	No public libraries using it and engaging in technical courses on it	1	YES	NO
120	UK	Daily Mail	"The safest way to stalk on Facebook: Social network adds Android app support for anonymity service Tor"	Reuters	January 2016	Facebook	Surveillance Circumvention	Private citizens	1	Facebook Website through Tor Network	1	–	0	NO	NO
121	USA	Penn Live.com	"Feds call former NSA contractor's theft of 50 terabytes of secrets 'breathtaking"'	Associated Press	October 2016	Harold Martin (former NSA's contractor)	Journalism & Whistleblowing	Private citizens, journalists, activists, state governments	0	Documents from the NSA	1	–	0	NO	NO

Continued on next page

Table – continued from previous page

#	Country	Newspaper	Article Title	Author	Year	Actor	Category	Peers	Auth.	Object	Ctrl.	Status Quo	Outc.	Effect on Reality	Rep. Art.
122	UK	The Guardian	"How to contact the Guardian securely"	The Guardian	September 2016	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	–	0	NO	NO
123	UK	The Guardian	"ProPublica launches world's first major news site on dark web"	Jasper Jackson	January 2016	ProPublica	Journalism & Whistleblowing	Private citizens, journalists, dissidents, activists, state goverments	1	World's first major news site in the Tor Network	2	–	0	NO	NO
124	UK	The Guardian	"Shari Steele on online anonymity: Tor staff are freedom fighters"	Bethany Horne	January 2016	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	–	0	YES	NO
125	USA	The NY Times	"Tor Project, a Digital Privacy Group, Reboots with a New Board"	Nicole Perlroth	July 2016	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	–	0	NO	NO
126	UK	The Guardian	"US defence department funded Carnegie Mellon research to break Tor"	Alex Hern	February 2016	Carnegie Mellon University	Digital Security	Private citizens, activists, state governments	1	Cybertools to attack the Tor Network	1	No FBI involvement in universities' research on Tor Network, no courtooms involved	1	YES	NO
127	UK	Daily Mail	"AlphaBay, the biggest illegal drugs marketplace in internet history, shut down by the Justice Department"	Hanna Parry	July 2017	Alphabay	Online Marketplace	Private citizens	−1	Marketplace Site	1	No drugs being traded over an online marketplace	1	YES	NO
128	UK	The Telegraph	"Canadian found dead in Thai cell wanted for running 'dark web' market"	Agence France-Presse	July 2017	Alphabay	Online Marketplace	Private citizens	−1	Marketplace Site	1	No Drug sellers benefiting from Online Marketplaces (having it easier)	1	YES	NO
129	UK	Daily Mail	"Canadian found dead in Thai cell wanted for running 'dark web' market"	AFP	July 2017	Alphabay	Online Marketplace	Private citizens	−1	Marketplace Site	1	Law and order: to not purchase illegal products; to not enrich through Tor online marketplaces	1	YES	NO
130	UK	The Guardian	"Computer security tips for whistleblowers and sources"	The Guardian	March 2017	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	–	0	NO	NO

Continued on next page

Table – continued from previous page

#	Country	Newspaper	Article Title	Author	Year	Actor	Category	Peers	Auth.	Object	Ctrl.	Status Quo	Outc.	Effect on Reality	Rep. Art.
131	USA	Oregon Live.com	"Dark web marketplace AlphaBay shut down by feds"	The Washington Post	July 2017	Alphabay	Online Marketplace	Private citizens	−1	Marketplace Site	1	Law and order: to not purchase illegal products; to not enrich through Tor marketplaces	1	YES	NO
132	UK	The Guardian	"Dark web marketplaces AlphaBay and Hansa shut down"	Samuel Gibbs and Lois Becket	July 2017	Alphabay	Online Marketplace	Private citizens	−1	Marketplace Site	1	Law and order: to not purchase illegal products	1	YES	NO
133	USA	The Washington Post	"Justice Dept announces takedown of AlphaBay, a dark Web marketplace for drugs and other illicit goods"	Matt Zapotosky	July 2017	Alphabay	Online Marketplace	Private citizens	−1	Marketplace Site	1	No overdoses and deaths from the purchase of online marketplace drugs	1	YES	NO
134	UK	The Guardian	"The dilemma of the dark web: protecting neo-Nazis and dissidents alike"	Alex Hern	August 2017	Tor Project	Surveillance Circumvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	Not helping dissidents' voices around the globe	1	YES	NO
135	UK	Daily Mail	"US, European police say dark web markets shut down"	AFP	July 2017	Alphabay	Online Marketplace	Private citizens	−1	Marketplace Site	1	To not trade illegal products	1	YES	NO
136	USA	AL.com	"What is Alphabay? Dark web site linked to heroin, Fentanyl sales seized, AG Sessions announces"	Leada Gore	July 2017	Alphabay	Online Marketplace	Private citizens	−1	Marketplace Site	1	To not trade illegal products	1	YES	NO
137	CHINA	Xinhua	"World's largest online 'dark market' shut down"	Chen Lidan, Bianji	July 2017	Alphabay	Online Marketplace	Private citizens	−1	Marketplace Site	1	To not trade illegal products	1	YES	NO
138	UK	The Guardian	"The ransomware attack is all about the insufficient funding of the NHS"	Charles Arthur	May 2017	Ransomware	Digital Security	Private citizens	1	Channel of communication and its storage (software)	2	No digital kidnaps and payments of rescue, specially hospitals	1	YES	NO
139	UK	The Guardian	"Share stories with us securely and confidentially"	The Guardian	December 2016	SecureDrop System	Journalism & Whistleblowing	Private citizens, dissidents, journalists, activists, state governments	1	Channel of communication and its storage (software)	1	–	0	NO	NO

Source: Author.