Barbara Idaerla Santos Calderon

REDE TOR E ATORES NÃO-ESTATAIS: UMA ANÁLISE DE DIFUSÃO DE PODER EM TRÊS DIMENSÕES

Dissertação submetida ao Programa de Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina para a obtenção do Grau de Mestre em Relações Internacionais.

Orientadora: Profª. Drª. Iara Costa Leite

Florianópolis
2018

Ficha de identificação da obra elaborada pelo autor
através do Programa de Geração Automática da Biblioteca Universitária
da UFSC.

Calderon, Barbara Idaerla Santos
Rede TOR e Atores Não-Estatais : Uma Análise de Difusão de Poder em Três Dimensões / Barbara Idaerla Santos Calderon ; orientador, Iara Costa Leite, 2018.
296 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro Sócio-Econômico, Programa de Pós-Graduação em Relações Internacionais, Florianópolis, 2018.

Inclui referências.

1. Relações Internacionais. 2. Difusão de Poder. 3. The Onion Router. 4. Dark Web. 5. Economia Política Internacional. I. Leite, Iara Costa. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Relações Internacionais. III. Título.

Barbara Idaerla Santos Calderon

REDE TOR E ATORES NÃO-ESTATAIS: UMA ANÁLISE DE DIFUSÃO DE PODER EM TRÊS DIMENSÕES

Esta Dissertação foi julgada adequada para obtenção do Título de "Mestre" e aprovada em sua forma final pelo Programa de Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina.

Florianópolis, 26 de junho de 2018.

_____
Prof. Helton Ricardo Ouriques, Dr.
Coordenador do Curso

Banca Examinadora:

_____
Prof.ª Iara Costa Leite, Dr.ª
Orientadora
Universidade Federal de Santa Catarina

_____
Prof. Marco Cepik, Dr.
Universidade Federal do Rio Grande do Sul (Videoconferência)

_____
Prof. Jaime Coelho, Dr.
Universidade Federal de Santa Catarina

_____
Prof. Gilson Geraldino Silva Júnior, Dr.
Universidade Federal de Santa Catarina

Este trabalho é dedicado aos meus pais.

AGRADECIMENTOS

Eu não poderia iniciar estes agradecimentos sem, sobretudo, agradecer extensamente ao Programa de Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina por ter confiado no tema desta pesquisa e permitido que eu pudesse ocupar uma das vagas do mestrado. Eu, igualmente, gostaria de agradecer a Universidade Federal de Santa Catarina por ter me oferecido, desde a graduação, ensino superior gratuito e de qualidade. Como cidadã brasileira, eu me empenho, diariamente, em fornecer à sociedade o retorno desta educação a mim concedida e que considero grande privilégio.

Agradeço também aos meus pais, Jorge e Japonaira, sem os quais nada disto seria possível. Meu pai, que desde pequena idade, me ensinou a relevância da educação para a vida em sociedade e soube, com paciência, mostrar-me o caminho das respostas para as dúvidas mais inquietantes. Como engenheiro, abriu-me os olhos para as ciências exatas: quando pequena, questões sobre a luz e buracos negros; quando adolescente, fórmulas matemáticas e a física da ficção científica; quando adulta, física quântica e universos paralelos. Minha mãe, desde muito cedo, conduziu-me ao caminho dos valores, propósitos e das emoções. Como professora, abriu-me os olhos para as ciências sociais: quando pequena, questões sobre o amor ao próximo e a família; quando adolescente, o valor do perdão e do convívio em sociedade; quando adulta, o aprendizado que deriva dos erros e o equilíbrio da liberdade. Eu sei que, onde quer que eu esteja, carregarei comigo traços de ambos – razão e emoção; exatidão e transbordamento; cérebro e coração. Obrigada por confiarem em mim e permitir-me sonhar tão alto quanto um pássaro, sem desconsiderar a importância da terra. Meus agradecimentos também se estendem aos meus irmãos Maggie e Júlio.

Devo agradecer a minha orientadora, Prof. Dra. Iara Costa Leite, por ter concordado em orientar-me em tema desafiador e ter mostrado-me os princípios do ator de pesquisar. Sua críticas relevantes conduziram me ao desenho desta dissertação. Sou muito agradecida por seu apoio, pelas reuniões que tivemos e experiência comigo compartilhada. Muito obrigada. Agradeço também ao prof. Dr. Gilson Geraldino Silva que compartilhou comigo um pouco de seu conhecimento estatístico e ofertou-me uma parte de seu tempo para que eu pudesse aprender um pouco mais. Isto mostrou-se fundamental para o caminhar desta pesquisa. Meus sinceros agradecimentos. Agradeço também ao prof. Dr. Jaime Coelho por participar como membro da

banca de defesa e retirar um pouco do seu tempo para leitura do trabalho e ofertar contribuições. Prof. Dr. Jaime, amigo desde os tempos da minha graduação, foi quem me permitiu, pela primeira vez, trabalhar com o tema que hoje segue. Obrigada mais uma vez. Meus agradecimentos também se estendem ao prof. Dr. Marco Cepik por, também, participar como membro da banca de defesa e, assim, dedicar tempo de leitura e brindar-me com críticas e contribuições. Sou bastante agradecida pela sua presença desde a banca de qualificação – momento importante para esta pesquisa pois permitiu-me refletir com paciência sobre suas colocações. Obrigada, professor.

Agradecimento especial aos meus queridos amigos da vida que, com bastante paciência, carinho e apoio, me proporcionaram um chão especialmente importante durante esta caminhada acadêmica. Vocês sabem quem são. Eu não poderia deixar de mencionar: Bianka Zimmer, sua importância e apoio não podem ser mensurados – minha melhor amiga, nos dias de chuva e sol, você sempre esteve lá e serei eternamente grata. Seu apoio diário foi fundamental para a produção desta dissertação e concretização de um sonho. Fernando de Bona Santiago, meu queridíssimo amigo que sempre me ofereceu apoio e a quem eu sei que posso contar para o que der e vier, que caminha nesta jornada comigo desde a graduação em Relações Internacionais pela UFSC e que, com maestria, sempre tem as melhores palavras pra acalmar um coração ansioso. Rulza da Silva, minha amiga há anos e quem sempre me proporciona conversas que me lembram o que é realmente importante na vida, muito obrigada, amiga minha. E à todos os demais que de alguma forma estiveram comigo nesta caminhada feliz e árdua: Ana Paula Althoff, sempre presente, longe ou perto; Camila Antunes da Luz, pelas noites de Masterchef que me trouxeram calmaria e bom-humor durante este trabalho; Luiz Fernando Guerreiro, meu amigo Loki, que sempre apareceu quando menos esperava-se e trouxe alegria e bom-humor no meio de conversas profundas sobre a vida; e a todos os meus outros amigos que de alguma forma me apoiaram durante esta pesquisa.

Agradeço também aos queridos amigos e colegas do prédio da pós-graduação que durante bom tempo dividiram o espaço comigo, as risadas, a alegria e o privilégio de aprender a pesquisar. Obrigada Lúcia da Secretaria, uma pessoa iluminada e que com bastante carinho ofertou aconchego, cafezinho e apoio a mim e todos os demais que, em algum momento, precisaram. Obrigada a Dona Bete que tornou as tardes mais divertidas e compartilhou comigo almoços e cafés. Agradecimento aos meus colegas de laboratório, Mamadou de Guiné Bissau, e meu ex-

veterano da graduação em RI, Júlio. Obrigada vocês dois pelas conversas instigantes e curiosas acerca do mundo social, pela companhia no laboratório (especialmente no período de férias acadêmicas) e, sobretudo, pelo apoio nesta jornada de pesquisa. Muito obrigada.

Obrigada aos meus amigos e colegas de mestrado que me apoiaram durante esta pesquisa e, principalmente, durante os dois anos em que recebi educação de qualidade neste programa de pós-graduação. Juntos nós crescemos, aprendemos, rimos e choramos com os prazeres e dissabores da vida acadêmica. Vocês contribuíram e foram essenciais para esta caminhada – marcaram este período de extenso aprendizado com as alegrias que surgem dos sonhos, anseios e expectativas. Obrigada aos queridos: Ana Luci, Alice Borba, Bruno Haeming, Karol Krespi, Diogo Oliveira, Guilherme Fasolin, Guilherme Mattos, Jonathan Hassel, Jozi Lawrence, Mari Almeida, Renan Jark, Roberta Prata, Terecita Gill, Tiago Mocellin, Tom dos Santos e Ricardo Kotz.

Finalmente, agradeço todos aqueles que direta ou indiretamente contribuíram para que esta pesquisa fosse realizada.

They are [these examples], 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 sure. That is the nature of exploration – and its appeal to the mentally adventurous.

(Susan Strange, 1996)

RESUMO

A difusão de poder foi um fenômeno primeiramente descrito por Susan Strange no contexto da Economia Política Internacional (EPI) em 1996. O fenômeno abarca em si os conceitos de poder relacional e estrutural, relevantes para o entendimento da disciplina de EPI. Embora descrito na década de 1990, a difusão de poder não discorreu acerca do domínio cibernético e muito menos, explicitamente, sobre as revoluções tecnológicas que culminaram com a rede mundial de computadores. No domínio do ciberespaço, diversos atores operam de modo a impor sua autoridade sobre indivíduos e serviços. Neste contexto, no começo do século XXI, surgiu a rede anônima de baixa latência "The Onion Router" que compõe a chamada "Dark Web", região do ciberespaço onde ocorre esforço ativo de blindagem da comunicação, privacidade e usuários específicos. Esta pesquisa busca, por meio de artigos jornalísticos publicados entre os anos de 2007 e 2017, analisar a difusão de poder na rede TOR em três dimensões: autoridade, controle e resultados.

Palavras-chave: Difusão de Poder. Dark Web. Rede TOR. Poder Estrutural. Poder Relacional. Economia Política Internacional.

ABSTRACT

The diffusion of power was a phenomenon firstly described by Susan Strange in the context of International Political Economy (IPE) back in 1996. The phenomenon encompasses concepts of relational and structural power relevant to the understanding of the IPE discipline. Although described in the 1990s, the diffusion of power did not address the cyber domain, much less explicitly the technological revolutions that culminated in the global computer network. In the domain of cyberspace, various actors operate in order to impose their authority on individuals and services. In this context, at the beginning of the 21st century, the low-latency anonymous network "The Onion Router" was created and it is part of the "Dark Web", a region of cyberspace in which there's an active effort to shield communication, privacy and users. This research seeks, through journalistic articles published between the years 2007 and 2017, to analyze the diffusion of power in the TOR network according to three dimensions: authority, control and outcomes.

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

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

BISA – British International Studies Association
CERN – Organisation Européene pour la Recherche Nucléaire
C&T – Ciência e Tecnologia
DARPA – Defense Advanced Research Projects Agency
DNS – Domain Name System
DW – Dark Web
EEF – Eletronic Frontier Foundation
EPI – Economia Política Internacional
EUA – Estados Unidos da América
FTP – File Transfer Protocol
GCHQ – Government Communications Headquarters
HTML – Hyper Text Mark-up Language
HTTP – Hyper Text Transport Protocol
IMAP – Internet Message Access Protocol
I2P – Invisible Internet Project
IP – Internet Protocol
IPEG – International Political Economy Group
IRC – Internet Relay Chat Protocol
ISIS – Islamic State in Iraq and Syria
ISP – Internet Service Providers
MIT – Massachussets Institute Technology
MTP – Message Transmission Protocol
MTP – Media Transfer Protocol
NCP – Network Control Protocol
NSA – National Security Agency
OIF – Organização Internacional da Francofonia
ONG – Organização Não-governamental
OP – Onion Proxy
OR – Onion Router
PDF – Portable Document Format
RI – Relações Internacionais
RSF – Repórteres sem Fronteiras
SI – Sistema Internacional
SMTP – Simple Mail Transfer Protocol
TCP – Transmission Control Protocol
TI – Tecnologia da Informação
TOR – The Onion Router
UNESCO – United Nations Educational, Scientific and Cultural Organization

UNIX – Uniplexed Information and Computing System
URL – Uniform Resource Locator
VOIP – Voice Over Internet Protocol
WARC – World Administering Radio Conference
WWW – World Wide Web

SUMÁRIO

INTRODUÇÃO

A presente pesquisa encontra-se em eixo de estudo ainda incomum dentro da disciplina de Relações Internacionais (RI): aquele que trata o domínio cibernético como o novo palco das ações entre diferentes atores no Sistema Internacional (SI). Este eixo encontra-se dentro de um guarda-chuva temático ainda mais abrangente que discute o papel da Ciência e Tecnologia (C&T) dentro da disciplina e busca compreender influências sobre os assuntos internacionais.

Autores expressaram a importância da C&T para as diversas dinâmicas abordadas pela disciplina de RI. (SKOLNIKOFF, 1993; WEISS, 2005; KRIGE; BARTH, 2006; MATTHEWS, 1997). Uns enfatizam que C&T é um poderoso e persistente fator, capaz de produzir alterações sociais e, assim, culminar nos assuntos internacionais (SKONILKOFF, 1993; MATTHEWS, 1997).[1] Outros apontam que esta relação também tem um sentido inverso – ou seja, quando a própria C&T são influenciadas pelos assuntos internacionais, direta ou indiretamente (WEISS, 2005, p.297). [2] Ou seja, do mesmo modo que os

[1] De fato, segundo Skolnikoff (1993), após o advento da segunda guerra mundial, e a descoberta de uma miríade de novidades científicas – inclusive, a descoberta da fissão nuclear pelo Projeto Manhattan norte-americano – qualquer dúvida sobre a relevância da tecnologia, para os propósitos do Estado, extinguiu-se. Nesta era, quase toda a tecnologia que o mundo venha a assimilar, ou lidar, é fruto de uma produção calculada de decisões tomadas em processos políticos existentes. Aliás, o próprio autor questiona quais aspectos, se é que existem, dos assuntos internacionais ainda não foram "tocados" pela C&T. Em especial, Skolnikoff (1993) aponta evidências da evolução da C&T nos assuntos internacionais: o envio massivo de forças nucleares estratégicas; o acidente nuclear de Chernobyl; as transações monetárias que ocorrem no exterior através de mercados financeiros digitais – que, em sua época, já ultrapassavam a casa dos 500 bilhões de dólares estadunidenses diários; e a quase total erradicação da varíola. Outra autora, Jessica T. Matthews (1997) em meados da década de 1990, apontava o relativo declínio dos Estados frente a ascensão de atores não-estatais no cenário mundial. Estes atores eram atores seriam "catapultados" ao palco global devido a revolução das telecomunicações e do computador – cujas consequências políticas e sociais, segundo ela, se mantiveram, até então, praticamente ignorados pela academia.

[2] Weiss (2005) aponta que os efeitos diretos podem ser sentidos de quatro modos: primeiro, a opinião pública afeta, de modo direto, o apoio público dados aos investimentos em C&T; segundo, os objetivos da política externa têm a capacidade de alterar as prioridades nacionais, realocando determinados investimentos em detrimento de outros; terceiro, o estado das relações entre dois países afeta a migração de cientistas, suas comunicações, colaborações, acessos a objeto de estudos, etc.; quarto, os acordos internacionais afetam a força global dirigida para a proteção da propriedade intelectual. Os efeitos indiretos operam através de mecanismos da Economia, Direito, Política e Cultura.

assuntos internacionais são influenciados pelo desenvolvimento tecnológico, o inverso também seria verdade.

Apesar da relevância do assunto para as RI, a literatura acadêmica sobre o mesmo é ainda limitada. Neste sentido, Eugene Skolnikoff apresenta-se como um dos grandes expoentes da área de convergência entre C&T e RI. Sua obra *The Elusive Transformation: science, technology and the evolution of international politics*, de 1993, tornou-se marco referencial no que tange as consequências das mudanças científicas e tecnológicas para a evolução da política internacional em diversas dimensões. Nesta obra, Skolnikoff (1993) também pondera sobre quais seriam as razões que levam a temática de C&T a ser negligenciada por acadêmicos das RI. Ele sugere, por exemplo, que os as informações e conhecimentos oriundos da C&T não são tratados com a importância devida porque a percepção, por parte dos estudiosos da área de RI, é de que são assuntos por vezes "obscuros". Esta obscuridade é a razão de serem relegados ao segundo, ou mesmo terceiro, plano.[3] Weiss (2005) complementa esta visão de dificuldade de assimilação: de acordo com ele, o tema de C&T, quando tratado pela área de RI, é abordado sem uma estrutura lógica definida. Como se o tema fosse composto, aparentemente, por tópicos residuais de outras temáticas da agenda de RI.

Na década de 1990, a revolução dos sistemas de informação, como ponto dentro da C&T, foi relevante aspecto de discussão acadêmica. No que diz respeito a autores que refletiram sobre a interface entre o tema e RI, destacamos quatro estudiosos: Strange (1988), Skolnikoff (1993), Builder (1993) e Nye (2011). Em comum, estes autores apontaram, indiretamente, de que modo as mudanças tecnológicas podem incidir sobre o poder do Estado.

Em 1988, antes da comercialização da Internet, a britânica Susan Strange publicou a obra *States and Markets* – que foi considerada ponto de partida para a compreensão do poder estrutural e, por esta razão, grande marco da literatura das RI e da Economia Política Internacional (EPI). Nesta obra, enquanto discursava sobre a estrutura do conhecimento, Strange (1988) ponderou sobre a revolução tecnológica que emergia ao final do século XX. Em especial, destacam-se três considerações acerca da mesma: (1) o desenvolvimento de sistemas de computadores sofisticados com alcance (disponibilidade e baixo custo)

[3] Skolnikoff comenta sobre isto quando afirma que "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)

acessível às massas; (2) a extensão dos sistemas de comunicação que utilizam satélites que orbitam o planeta; (3) e o aspecto da digitalização da linguagem que, em grande medida, diminui as barreiras linguísticas que separam os grupos humanos. Em geral, Strange (1988) traçou apontamentos acerca da revolução tecnológica e suas implicações sobre a provisão e o controle da informação e dos sistemas de comunicação. Ela também apontou mudanças no uso da linguagem e canais de comunicação não-verbais; em percepções que considera fundamentais sobre as condições humanas que influenciam julgamentos e, através deles, políticas e decisões políticas e econômicas. Estes pontos são fundamentais para compreender a dinâmica da estrutura do conhecimento, difusão de poder e a incidência destes elementos sobre o poder do Estado.

Outro estudioso, Eugene Skolnikoff, em 1993 – no período limiar da abertura comercial e global da rede mundial de computadores –, não deixou de ponderar sobre as tecnologias da informação. Embora não tenha versado, explicitamente, sobre a Internet e suas implicações para a política internacional, ele discorreu sobre a relevância das recentes mudanças tecnológicas sobre o poder político. Segundo ele, a introdução das tecnologias de informação aumentaria, consideravelmente, as limitações de centralização do poder político.[4] Para Skolnikoff (1993), esta conclusão é tão amplamente aceita entre os comentaristas de política internacional que as análises dos assuntos internacionais, em grande medida, referem-se às tecnologias da informação como fatores-chave que, indiscutivelmente, proporcionariam mudanças no sistema internacional. (SKOLNIKOFF, 1993). No entanto, ele deixa claro que não ocorrerá, em razão disso, a dissolução do Estado ou diminuição de sua relevância no SI.

No limiar da abertura comercial da Internet, Carl H. Builder foi outro autor que contribuiu para as análises sobre o impacto da revolução dos sistemas de informação sobre as relações internacionais. Segundo Builder (1993), parte do entusiasmo sobre a nova era da informação advém das possibilidades que a exploração do hardware oferta em relação ao poder. Esta era, responsável por encurtar os espaços do globo terrestre, difundiu uma nova perspectiva sobre o poder calcado na

[4] Especialmente sobre essas limitações, ele afirma que "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).

informação. Para Builder (1993), o Estado encontra-se diante de um dilema: permitir, ou negar, a livre comunicação a partir dos novos sistemas de informação? A permissão traria como consequência a concessão do poder da informação aos indivíduos. E, de posse deste poder, os mesmos teriam capacidade suficiente para desafiar diversas hierarquias que foram, elas próprias, instauradas e mantidas a partir da lógica de controle e negação à informação. Por outro lado, a negação do acesso à comunicação, e às tecnologias oriundas desta nova era da informação, poderia significar a perda da chance de inserir-se, de modo sólido, na economia global.[5]

Finalmente, em 2011, o reconhecido acadêmico de RI, Joseph Nye Jr., publicou a obra *The Future of Power*, no qual discorreu sobre a relevância da nova era da informação para as novas considerações sobre o poder. Nesta obra, Nye realiza ponderações sobre as revoluções tecnológicas do final do século XX e o modo como proporcionaram o surgimento do novo poder, denominado por ele de "Cyberpower". É neste cenário de regime híbrido – em que a realidade concreta de cabos, máquinas, computadores, satélites e demais infraestrutura, se mescla com a abstração virtual de bytes digitais e interações de agentes – que se produz o tecido do novo domínio no século XXI: o ciberespaço. Neste âmbito, o Estado e novos atores surgem para buscar espaço e competir por poder. (NYE, 2014). Contudo, ele sugere cautela ao considerar o poder neste domínio, pois o ciberespaço não substituirá o espaço geográfico e nem extinguirá a soberania do Estado. (NYE, 2010).

Em suma, os autores supracitados, apesar de realizarem considerações relevantes sobre as mudanças tecnológicas em curso ao final do século XX sobre o poder do Estado, foram cautelosos em afirmar que tais alterações não significam a diminuição da relevância do Estado no SI, ou sua extinção.

---

[5] Builder (1993) também trata de outros pontos relevantes sobre o tema. Um de seus questionamentos acontece em torno da aparente "revolução" da informação que atinge o final do século XX: o mundo estaria diante uma transição ou revolução? Caso fosse uma transição, esta transição é entre uma sociedade com relativa pobreza de informação para uma sociedade com relativa abundância de informação. Sendo assim, esta transição surtiria efeitos revolucionários sobre todas as instituições e hierarquias já edificadas. No entanto, se o mundo está diante de uma revolução, as vítimas mais óbvias desta dinâmica são os Estados-nacionais e seus governos. Não que fossem desaparecer, mas dariam lugar a novos atores. Sendo assim, uma importante consequência desta nova era da informação é a emergência de facções transnacionais. Semelhante à Strange (1996), Builder (1993) também discute sobre o poder concentrado no Estado-nação e sua consequente difusão para novos atores não-estatais.

Se, antes da comercialização e uso massivo da Internet, já se discutia a necessidade de incluir o tema de C&T no leque de assuntos pertinentes à área das RI, atualmente tal necessidade é preponderante. [6] Existe a necessidade de que parte dos esforços de pesquisa concentre-se no campo de intersecção entre os Sistemas de Informação, Ciência e Tecnologia, e Relações Internacionais – tendo em vista o desenvolvimento do tema e relevante interesse público, sobretudo, no rol de assuntos que têm como foco o ciberespaço. Este último, aliás, tem incutido implicações políticas e econômicas relevantes o suficiente para reverberar em pesquisas de diferentes áreas de estudo que tangenciam temas da agenda de RI.

Em se tratando de pesquisas e investigações na área de RI e o ciberespaço, os temas variam bastante. Algumas pesquisas se concentram na dimensão tecnológica do sistema de Vestfália na era da Internet. (BRUNN, 1998; MILLS, 2012; TIKK-RINGAS, 2012; DEIBERT, 2013; DEMCHAK; DOMBROWSKI, 2013). Outros estudos buscam compreender as RI através do olhar característico das Tecnologias da Informação (TI) – seja de modo a analisar a convergência da "era digital" e a "era do terror" (DERIAN, 2003); seja de modo a incidir sobre o papel do Estado, atores privados e comércio online diante da regulação dos fluxos de informações (FARRELL, 2006). Muito, inclusive, tem se discutido sobre a governança digital – com especial destaque às investigações de Canabarro (2014). Outros pesquisadores defendem uma visão das Relações Internacionais dentro do domínio cibernético a fim de investigar a governança digital. (VAISHNAV; CHOUCRI, 2013; MUELLER; SCHMIDT, 2013). E, ainda, existem aqueles que discutem o papel da rede mundial de computadores diante das questões diplomáticas e de política externa. (ROSS, 2011). Afinal, sendo a política uma ação que está ligada às atividades dos atores no contexto coletivo, muito se pondera sobre as atividades políticas destes atores no domínio cibernético. (CASTELLS; CARDOSO, 2005; ROCHE; BLAINE, 2014; SIEDLER, 2016). Sobretudo, talvez os assuntos mais investigados sejam dois: cibersegurança (NISSENBAUM, 2005; NYE, 2011; CHOUCRI; GOLDSMITH, 2012; KALLBERG; THURAISINGHAM, 2012; KRAMER, 2012; HATHAWAY, 2012; CEPIK; CANABARRO; BORNE, 2014) e guerra cibernética. (BERENGER, 2006; WALSH; BARBARA, 2006; MICHALSKI; GOW, 2007; CLARKE; 2009;

[6] Eugene Skolnikoff (1993) talvez seja o maior expoente dessa agenda que preza pela inclusão da tecnologia nos assuntos da disciplina de Relações Internacionais.

LIBICKI, 2009; CORNISH et al, 2010; LAWSON, 2012; HURWITZ, 2013; JUNIO, 2013; CEPIK; CANABARRO; BORNE, 2015; JAJODIA et al, 2015; SCHREIER, 2015; SCHNEIDER, 2016). Há, sobretudo, uma expressiva lacuna no que tange o estudo da Dark Web e RI, temas desta dissertação.[7]

Esta pesquisa preocupa-se com a estrutura do conhecimento no contexto do domínio cibernético. Em especial, busca averiguar evidências da difusão de poder a partir da rede anônima de baixa latência "The Onion Router" (TOR) – componente da Dark Web. Esta última é parte peculiar, e com definição própria, da rede mundial de computadores. Sendo assim, adotamos o campo da EPI, sob o viés de Strange (1988, 1996), como marco teórico de análise do estudo por acreditar que esta corrente tenha elementos suficientemente capazes de explicar o fenômeno da difusão de poder no domínio cibernético de modo a abranger, tanto a pluralidade de atores, quanto o contexto digital de atuação dos mesmos.

1.1 DELIMITAÇÃO DO TEMA E PERGUNTA DE PESQUISA

Na obra de 1996, *The Retreat of the States: the diffusion of power in the world economy*, Susan Strange explicita que o poder estrutural pode ser observado a partir de um quadro analítico que define "who-gets-what" na sociedade global baseado em quatro estruturas básicas: estrutura da segurança, estrutura da produção, estrutura das finanças e estrutura do conhecimento.[8] De modo resumido, o objetivo da obra é

[7] No banco de dados da SCOPUS – maior banco de dados de "abstracts" e "citações" de literatura revisada pelos pares, de acordo com a própria –quando o usuário realiza uma pesquisa utilizando o código "dark web", restringindo as áreas de "social sciences", "decision sciences", "business, management and accounting", "economics, econometrics and finance", "multidisciplinary" e "arts and humananities", ou seja, áreas que tangenciam RI, a pesquisa confere um retorno de 38 ocorrências. Quando, em vez de "dark web", utiliza o código "tor network", o resultado é de 24 ocorrências. Ou seja, o total é de 62 documentos. Quando restringimos as áreas de "computer science", "engineering" e "mathematics", utilizando o código "dark web", são 87 resultados. O código "tor network" nos fornece 165 documentos. No total, são 252 documentos – mais de quatro vezes os resultados das áreas sociais.

8 Dentro de cada uma destas estruturas, o poder sobre os demais – e também sobre a mistura de valores do próprio sistema – é exercido dentro e fora das fronteiras dos Estados-nacionais por: (1) aqueles que estão em posição de ameaçar ou oferecer segurança; (2) aqueles que estão em uma posição de recusar ou oferecer crédito; (3) aqueles que definem o que é

atrair a atenção para o poder, que origina-se a partir destas estruturas, de atores não-estatais. Em razão deste poder, tais atores têm capacidade de alterar os resultados no SI. O poder estrutural, definido por Strange (1988), é derivado, e está condicionado, por estas quatro estruturas.

Através deste quadro analítico sobre a natureza do poder, a autora logrou separar-se das correntes tradicionais da disciplina de RI que sustentavam a posição do Estado-nação como ator principal do SI – e, de acordo com ela, muitas vezes único.[9] Strange (1996), por sua vez, busca argumentar a existência e relevância de outros atores além do Estado para a política e a economia global: organizações internacionais, corporações transnacionais, profissões transnacionais, empresas multinacionais, etc.

O foco de nossa pesquisa é a análise da difusão de poder no contexto da rede anônima TOR, inserida no domínio cibernético. Pela natureza desta rede, a difusão de poder assenta-se sobre a quarta estrutura definida por ela – estrutura do conhecimento. Acerca do poder e desta estrutura, Strange (1988) afirmou que

> 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).

Em se tratando do domínio cibernético, que surge ao final do século XX, é possível averiguar a existência de uma multiplicidade de

---

produzido, onde, por quem e sobre quais condições e termos; (4) aqueles que controlam o acesso ao conhecimento e à informação, e também aqueles que estão em posição de definir a natureza do conhecimento. (STRANGE, 1996).

9 Em especial o Realismo que, sob suas diferentes vertentes, observa o Estado-nação como detentor de poder nas relações nternacionais – seja através da concepção de poder relacional ou poder material.

atores que utilizam a Internet para dar cabo a suas atividades. Nesta Internet pública, livre de restrições e ausente de tecnologias que forneçam privacidade e anonimato aos usuários e suas comunicações, as denúncias sobre a vigilância realizada por parte de empresas e entidades governamentais ganham contornos na voz de ativistas e denunciantes. (LANDAU, 2013; SCHEUERMAN, 2014; BAKIR, 2015; WALSH, MILLER, 2015; MURATA, ADAMS, PALMA, 2017). Por esta razão, a rede de baixa latência TOR – que busca prover privacidade e anonimato de usuários e comunicações utilizando a rede mundial de computadores – insere-se no debate sobre vigilância e privacidade na era digital como um importante canal de comunicação. E é, por meio da Dark Web, na figura da rede TOR, que diversos atores realizaram operações políticas que reverberaram na mídia jornalística dos tempos recentes e se tornaram conhecidos do público geral. Para ilustrar este ponto, citamos: o grupo WikiLeaks, de Julian Assange (WIKILEAKS, 2016); o grupo "hacktivista" Anonymous (COLLEMAN, 2011); a organização transnacional Repóteres Sem Fronteiras (REPORTERS WITHOUT BORDERS, 2016); o ex-agente da National Security Agency (NSA), Edward Snowden – que utiliza a rede TOR, além de outros mecanismos, para blindar suas comunicações e adquirir privacidade (LEE, 2015); o grupo terrorista Al-Qaeda (COHEN-ALMAGOR, 2012); o mercado negro das drogas Silk Road (CHRISTIN, 2012); moedas criptográficas como a BitCoin, largamente utilizada em transações comerciais nas redes anônimas da Dark Web (KUHN, 2015); e, em menor medida, terroristas jihadistas e pedófilos (MOORE; RID, 2016).

Visto que, de acordo com Strange (1988), a estrutura do conhecimento compreende os canais através dos quais crenças, ideias e conhecimento são comunicados, é razoável investigar a difusão de poder na rede TOR e os atores que operam o poder por esta via. Sendo assim, elaborou-se a pergunta de pesquisa que buscou compreender como, e em que medida, a rede TOR aumenta a difusão de poder estrutural no século XXI. O objetivo desta pesquisa é investigar a questão da difusão de poder, nesta região do ciberespaço, averiguando evidências do aumento (ou diminuição) de poder por parte de agentes não-estatais. Tais evidências devem, sobretudo, ser amarradas por resultados na dimensão real geográfica do SI.

1.2 JUSTIFICATIVAS

São seis justificativas básicas que fundamentam a escolha do tema e o recorte da presente pesquisa. Em primeiro lugar, a ascensão da temática "cyber" como nicho de estudo para RI. Em segundo, a urgência do tema de redes anônimas no debate acerca da vigilância digital global perpetrada por entidades governamentais e corporativas. Terceiro, justifica-se a escolha da estrutura do conhecimento em detrimento das demais estruturas abordadas por Strange (1988) – segurança, produção, finanças. Quarto, as possíveis contribuições acadêmicas desta pesquisa para os estudos de difusão de poder na área de EPI e RI. Quinto, justifica-se também a escolha da rede anônima de baixa latência TOR, as mídias jornalísticas selecionadas e os atores apresentados nesta pesquisa. Por último, as motivações pessoais da autora sobre as escolhas e recortes realizados.

Primeiro, a ascensão da temática "cyber" ocorre, principalmente, a partir do novo milênio. O final do século passado proporcionou mudanças de paradigmas tecnológicos, políticos e sociais em diferentes dimensões. De acordo com Castells e Cardoso (2005), este século foi responsável por "catapultar" a vida humana em direção a uma nova fase em termos tecnológicos. O período que abrange as mudanças relevantes ao "salto" tecnológico vivido pela sociedade é conhecido pela literatura como a "Era da Informação" ou da "Sociedade em Rede". Esta última, por definição, "[É] a estrutura social que resulta da interação entre o novo paradigma tecnológico e a organização social como um todo". (Ibid., p.3). Existe um elemento inédito nesta sociedade que é a "base microeletrônica da tecnologia em rede que provê novas capacidades para uma antiga forma de organização social: em rede." (Ibid., p.4). Em outras palavras, o homem não apenas utilizava as redes de comunicação, anteriores ao século XX, como eram bastante comuns. O ineditismo acontece pelo caráter das ligações da rede, atualmente calcadas no digital e com alcance, de fato, global.10 (Ibid., p.4)

Faz-se necessário reconhecer que, ao final do século XX, surge um terreno novo que não é adequadamente abraçado pela área de RI – embora tenha alcance global, caráter social e econômico. No entanto, mesmo que não tenha o mesmo volume de estudos que áreas tradicionais da disciplina, avanços consideráveis têm tido êxito – como apontado anteriormente nesta pesquisa. Uma das razões para a temática "ciber" ter

10 Castells e Cardoso (2005) fazem uma pequena ressalva: apesar de considerada global, esta sociedade em rede é difusa e apresenta um elemento de exclusão por não incluir a totalidade da humanidade.

conquistado maior espaço dentro do escopo das ciências sociais – embora seja relativamente menor que as ciências naturais – foi a publicação, em junho de 2013, pelo jornal britânico The Guardian, de um conjunto de reportagens que se tornaram conhecidas como as "Revelações Snowden" e cujo conteúdo reverberou em diversos países simultaneamente. As informações detalhadas pelo jornal foram fornecidas, através de documentos secretos, por Edward Snowden, empregado da empresa Booz Allen Hamilton que prestava serviços para a NSA – agência de segurança nacional dos Estados Unidos da América (EUA). Segundo Landau (2013) os documentos fornecidos evidenciavam diversos esquemas de vigilância e espionagem tendo como foco a Internet.11 A partir das Revelações Snowden, a comunidade acadêmica publicou alguns estudos acerca do tema sob diferentes óticas. (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; GURSES, KUNDNANI, HOBOKEN, 2016; MURATA, ADAMS, PALMA, 2017). Castells e Cardoso (2005) afirmam que a Sociedade em Rede configura-se, atualmente, como núcleo das sociedades em curso. Por esta razão, torna-se imperioso que novos estudos sejam realizados na temática "cyber".

Em segundo lugar, temas relativos a manutenção de direitos e liberdades civis que possam assegurar a privacidade, o consentimento e a livre-expressão na Internet ganharam novos contornos após as massivas revelações sobre vigilância digital perpetrada pelos EUA através da Internet.12 Após o vazamento dos documentos secretos,

11 Landau (2013) explicita alguns: o programa de coleta doméstico de metatados das telecomunicações da Verizon Business Networks Services – incluindo o "quem", "o que", "quando" de chamadas telefônicas; o programa "PRISM", da NSA, que visava as comunicações específicas da Internet e armazenamento de dados de pessoas fora das fronteiras dos Estados Unidos e daqueles com as quais elas se comunicam; a extensão da cooperação de empresas privadas norte-americanas com o governo dos Estados sobre o fornecimento de dados de usuários e clientes; informações sobre a espionagem norte-americana sobre computadores chineses; a operação conjunta entre NSA e a Government Communications Headquarters (GCHQ), a contrapartida britânica de agência de segurança, para monitorar as comunicações de líderes políticos atendentes da Cúpula do G20 em Londres de 2009; a condução de esquema de vigilância em massa por parte dos britânicos; o esquema de coleta de metadados de comunicações domésticas da Internet, entre outros. Lucas (2014) adiciona outros: o programa "XKeyscore", revelado em julho de 2013; o programa de encadeamento de dados, "Enterprise Knowledge System".

12 A organização sem-fins-lucrativos, Electronic Frontier Foundation (EFF), fundada em 1990, é líder na defesa das liberdades civis no mundo digital e, atualmente, batalha na justiça

Snowden, vivendo em exílio na Rússia, passou a advogar por privacidade, encriptação e por uma reforma robusta do sistema de vigilância atuais. (LEE, 2015). A privacidade e o anonimato na Internet, constantemente, são defendidos de modo aberto pelo ex-agente da NSA. Neste sentido, a rede anônima TOR foi elevada por ele à categoria de mais importante tecnologia de melhoria da privacidade online da era atual. (Ibid., 2015). O posicionamento político de Snowden não se limita ao desejo de privacidade apenas aos cidadãos comuns. Pelo contrário, ele advoga por demais membros da sociedade: desde aqueles circunscritos em regimes autoritários aos profissionais que têm compromisso com a reportagem e precisão dos fatos, incluindo dissidentes políticos, denunciantes, ativistas, etc. Apesar das ações destes sujeitos serem realizadas no campo abstrato do ciberespaço, suas consequências têm implicações para a realidade concreta. Isto demonstra o caráter político do canal de comunicação TOR no século XXI. Compreender seu funcionamento, bem como as ações de diversos agentes que nele operam, permite examinar de que modo as relações de poder configuram-se no campo digital hoje – e, mais uma vez, com implicações na realidade concreta.

Terceiro, nossa abordagem visa a análise da difusão de poder no contexto da rede anônima TOR. Esta rede insere-se, por definição, na estrutura do conhecimento visto que é esta estrutura que lida com "the channels by which beliefs, ideas and knowledge are communicated – including some people and excluding others." (STRANGE, 1988, p.119). Por essa razão, e por fins de recorte de pesquisa, analisaremos a difusão de poder a partir desta estrutura. É importante, portanto, compreender o foco da nossa análise e as origens do poder estrutural – são pontos distintos. Enquanto o foco de análise da difusão de poder desta pesquisa recai sobre a estrutura do conhecimento – que, acreditamos, mais tem condições de explicar a realidade da rede TOR e dos atores que nela atuam –, o poder estrutural, tal como concebido por Strange (1988), continua sendo fruto que deriva a partir das quatro estruturas primárias, em maior ou menor grau. Assim, acreditamos ser possível que o foco da análise seja sobre uma das estruturas, sem prejuízo de significados conceituais. A própria autora, por vezes, dedica

---

norte-americana contra a NSA em razão da vigilância perpetrada por esta última sobre a infraestrutura da Internet. (TUMMARELLO, 2016). Na justiça, a EFF afirma que a NSA viola a quarta emenda constitucional dos EUA ao copiar e procurar por dados coletados do backbone12 da Internet nosEUA.(MAAS, 2014).

o foco de análise a estruturas diferentes quando versa sobre difusão de poder.13

Quarto, acreditamos que a presente pesquisa contribua para os estudos acadêmicos acerca do tema da difusão de poder de duas formas: primeiro, por trazer a temática para o contexto cibernético; e, segundo, por operacionalizar o conceito de modo a auxiliar as análises sobre o tema da difusão. As duas obras de Strange (1988, 1996) não trouxeram variáveis que pudessem, ao menos, balizar o direcionamento das análises sobre difusão de poder – de que modo ela ocorre e em que medida. Acreditamos que a construção de variáveis que pudessem, ao menos, demarcar a análise, seja relevante. Portanto, trabalharemos com três variáveis durante nossa investigação sobre difusão de poder no contexto da rede anônima de baixa latência TOR: autoridade, controle e resultados. A metodologia que as envolve será descrita na seção metodológica desta introdução.

Quinto, justificamos a investigação sobre a rede TOR, as mídias jornalísticas selecionadas e os atores apresentados nesta pesquisa. No contexto das redes que compõem a Dark Web, a rede TOR é considerada a maior em número de nódulos e usuários, além de ser percebida como aquela que possui tecnologia criptográfica mais sofisticada. (MOORE; RID, 2016, p.15). Além disso, buscamos utilizar mídias jornalísticas alternativas em formato de jornal online para compor o banco de dados sobre os quais operamos as variáveis descritas acima. A seleção destes jornais ocorreu por meio do rank Top 10 Online Newspapers Worldwide Ranked by Unique Visitors (000), de 2012, cuja fonte é atribuída à ComScore, empresa norte-americana sediada na Virgínia, que realiza diferentes análises relativas ao domínio da Internet. (COMSCORE, 2012). Finalmente, os agentes selecionados para análise das três variáveis foram aqueles que: (1) poderiam ser considerados como pertencentes à estrutura do conhecimento, segundo definição de Strange (1988); (2) atores cujas operações ocorreram por meio da rede anônima TOR.

A sexta e última justificativa relaciona-se com motivações pessoais da autora. Tais motivações resume-se à afinidade com a

13 Por exemplo, Strange (1996) dedica o foco de análise sobre a Máfia italiana na estrutura da segurança. A máfia rivaliza com o Estado italiano por posicionamentos dentro da estrutura da segurança. Do mesmo modo, admite que o poder estrutural de posse da Máfia é derivado, em maior ou menor grau, das quatro estruturas – seja pelo fornecimento de proteção física a membros e aliados; seja pela comercialização de produtos e serviços ilícitos; fornecimento de crédito a interessados; acesso à conhecimento e redes de informação; etc.

temática da computação, dos sistemas de informação e da tecnologia em geral. Durante a infância, aprendeu linguagens computacionais e pôde, pela primeira vez, construir um website na WWW. Esta aproximação a inseriu nos estudos da Ciência da Computação, que não foram finalizados em razão do ingresso ao curso de Engenharia Civil. O interesse e afinidade com as Ciências Exatas são de longa data. Ambas as áreas foram deixadas de lado quando principiou, e finalizou, a graduação em Relações Internacionais na Universidade Federal de Santa Catarina, tornando-se bacharela em fevereiro de 2015. Seu Trabalho de Conclusão de Curso (TCC), apesar de curto, teve como tema a "Deep Web" e a "Dark Web". O TCC sustentou-se em três justificativas: o latente interesse em Tecnologia e Sistemas da Informação, em especial o universo da Internet; os movimentos ativistas do domínio cibernético como grupo Anonymous, WikiLeaks, Tor Project e as revelações de Edward Snowden acerca da vigilância global das comunicações perpetradas pelos membros do Cinco Olhos ("Five Eyes") que tiveram implicações políticas para o cenário internacional; e, finalmente, as preocupações crescentes em torno da marginalização destes conteúdos dentro da área de RI. Em 2016, ingressou no Programa de Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina com a proposta de continuação dos estudos na área da Difusão de Poder e Dark Web. Em 2017, lançou pela editora Alta Books, livro intitulado "Deep&Dark Web: a Internet que você conhece é apenas a ponta do iceberg".

A presente pesquisa é, sobretudo, uma tentativa de análise das forças e movimentos que ocorrem no domínio cibernético e que reverberam na política econômica internacional e no cotidiano de milhões de pessoas ao redor de todo o mundo.

1.3 OBJETIVOS

Esta dissertação trabalha com um objetivo geral e cinco objetivos específicos.

1.3.1 Objetivo Geral

O objetivo geral da pesquisa é compreender como, e em que medida, a rede TOR aumenta a difusão de poder estrutural no século

XXI. Para viabilizar o alcance deste objetivo geral, propõem-se os seguintes objetivos específicos.

1.3.2 Objetivos Específicos

(a) Examinar o aspecto teórico do poder estrutural que o faz divergir, fundamentalmente, das abordagens tradicionais sobre o poder em RI;

(b) Propor a operacionalização do conceito de difusão de poder, elaborado por Strange (1996), por meio de três variáveis qualitativas ordinais;

(c) Descrever os aspectos históricos, teóricos e tecnológicos que sustentam e acomodam a rede anônima TOR no universo do ciberespaço e a distingue de outros canais de comunicação;

(d) Analisar o banco de dados – composto por sujeitos da estrutura do conhecimento selecionados por meio de artigos de jornais – de modo a atribuir valores às variáveis representativas das três dimensões do poder que atestam sua difusão;

(e) Avaliar, por meio dos objetivos específicos anteriormente descritos, de que modo e em que medida a rede TOR aumenta a difusão de poder no século XXI.

1.4 METODOLOGIA

O ponto de partida metodológico desta dissertação é a revisão de literatura. Inicialmente, partimos de uma visão holística sobre o tema de **Ciência, Tecnologia e Relações Internacionais** e o posicionamento desta pesquisa no contexto do tema supracitado. Na sequência, mapeamos a discussão sobre **Internet e Relações Internacionais** de modo a investigar os assuntos já pautados por estudiosos da área sobre o domínio cyber e correlacionar com esta pesquisa (exposto na introdução desta dissertação). Nós realizamos uma extensa busca sobre **Poder e Relações Internacionais** de modo a examinar de que modo o marco

teórico, relativo ao poder, configura-se como abordagem dentro da disciplina. Em seguida, observamos como o elemento **Difusão de Poder** é tratado pelo marco teórico e demais autores da área – de modo a traçar distinção e similaridades. O tema desta pesquisa, referente a Dark Web, encontra-se pautado no ciberespaço e, por esta razão, buscamos identificar a rede mundial de computadores como domínio próprio. Para isso, buscamos na literatura a **Origem da Internet** atual, no que tange o seu aspecto técnico, modo a reunir conhecimentos sobre sua operacionalização e funcionamento. Logo, compreendemos a partir da literatura sobre **Deep Web** as diferentes nuances da World Wide Web, dentre as quais a Dark Web configura-se como apenas uma das categorias. Finalmente, para fins de compreensão da especificidade e natureza tecnológica da rede anônima de baixa latência TOR, nós examinamos a literatura sobre **Dark Web e TOR** de modo a fornecer os insumos básicos por meio dos quais realizamos a análise de difusão de poder.

Segue abaixo quadro composto pela revisão de literatura.

QUADRO 1 - REVISÃO DE LITERATURA	
CATEGORIAS	**LITERATURA SOBRE O ASSUNTO**
Ciência, Tecnologia e Relações Internacionais	SKOLNIKOFF, 1993; WEISS, 2005; KRIGE; BARTH, 2006; MATTHEWS, 1997; BUILDER, 1993.

Internet e Relações Internacionais	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; TIKK-RINGAS, 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, CHARTERIS-BLACK, 2015; LYON, 2015; MERCK, 2015; NOCETTI, 2015; QIN, 2015; SALVO, NEGRO, 2015; GURSES, KUNDNANI, HOBOKEN, 2016; MURATA, ADAMS, PALMA, 2017; TUMARELLO, 2016; CASTELLS, 2001.
Poder e Relações Internacionais	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;

Difusão de Poder	BUILDER, 1993; NYE, 2011.
Origem da Internet	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 e 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.

O marco teórico desta dissertação são as obras escritas pela britânica Susan Strange que versam direta e indiretamente sobre o fenômeno da difusão de poder: *States and Markets*, 1988; *The Retreat of the State*, 1996. A partir do marco teórico, surgiu a necessidade de sistematização de seu conteúdo na forma de três dimensões distintas e

complementares que compõem o fenômeno de difusão de poder: autoridade, controle e resultados. Estas dimensões encontram-se presentes de modo implícito nas obras – mas não como dimensões propriamente ditas, e sim como elementos relevantes para a composição do quadro analítico por meio do qual solidifica-se a visão global de economia política da autora. A difusão de poder é um fenômeno que ocorre, separadamente, em cada uma das três dimensões.

O elemento "autoridade" é interpretado à luz da concepção de poder. Em raras ocasiões Strange (1996) utiliza o termo "poder" quando discute o fenômeno da difusão de poder, preferindo o termo "autoridade". Ao examinar o termo "autoridade" na obra, nós percebemos que existe uma dualidade interpretativa relacionada a ele: em algumas ocasiões o termo é visto como a própria instituição, entidade, sujeito que reúne em si a expectativa do poder (ser autoridade); em outras ocasiões o termo é observado como sinônimo de poder, ou melhor, com a capacidade de afetar os resultados de modo a impor as preferências do sujeito (exercer autoridade). Nós buscamos fundamentar no primeiro capítulo as razões que nos indicam a existência desta dualidade interpretativa, além de realizar considerações mais detalhadas sobre o modo como estas "autoridades" ocorrem.

Nesta dimensão, insere-se os discursos da autora em relação aos efeitos do poder oriundos da presença ou envolvimento de uma autoridade – sem a necessidade de agir, operar, realizar atividades. Especialmente em suas obras, Strange (1996) argumenta que esta noção sobre o poder encontra origens nas abordagens feministas. Dentro de um determinado contexto, a presença de uma figura compreendida como autoridade pode ser representativa do poder – e produz efeitos que são sentidos e percebidos pelas demais figuras neste contexto, acarretando consequências. Para ilustrar, a autora aborda as relações sobre homens e mulheres e o poder inrerente da presença masculina no contexto social.[14]

14 Especialmente sobre esta noção de que o poder pode agir apenas por presença, e não apenas oriundo de ações, ela realiza algumas considerações acerca deste poder que discute ser "estrutural", ou melhor, que é produto da dinâmica de estruturas estabelecidas (inclusive no caso da abordagem feminista, uma vez que o poder origina-se a partir da dinâmica estrutural estabelecida no contexto social do "machismo"): "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

Além disso, a presença da autoridade pode emanar dos seus pares reconhecimentos de três cenários possíveis: que a autoridade está mais "forte", que permaneceu a mesma, ou que tenha "enfraquecido".[15] Abordaremos em detalhes estas ideias no capítulo um, seção que versa sobre a dimensão da autoridade.

O "controle" é um elemento que surge com especial frequência nas obras de Strange (1988, 1996) quando trata-se da operacionalização de objetos dentro das estruturas primárias. Em algumas ocasiões, é dito por ela que os atores posicionados nas estruturas primárias têm poder quando controlam algum aspecto relevante para a influência dos resultados no cenário econômico-político. (Ibid., 1988). E o possessor do controle do objeto que influencia os resultados não necessariamente é a autoridade. Como meio de fundamentar a existência da dimensão controle, no primeiro capítulo nós identificamos em diversos exemplos mencionados pela autora atores posicionados dentro da estrutura

---

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 A percepção dos pares sobre a autoridade (se é crescente, decrescente ou indiferente) é uma ideia indiretamente trabalhada na obra de 1988. Sobre isso, podemos extrair alguns exemplos formulados pela própria autora: "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 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 indispensible but it could only be used to affect outcomes in conjunction with military capability and economic resources." (STRANGE, 1988, p.32)

primária e o objeto de seu controle que é considerado relevante para influenciar os resultados.

Os "resultados" são fundamentais em sua literatura porque são eles que determinam a autoridade e o controle dos atores: a alteração do status-quo indica poder; enquanto que sua não-alteração, por vezes, pode indicar ausência de poder.[16] A dimensão "resultados" abarca tanto o poder estrutural, de modo indireto, quanto o poder relacional, de modo direto.

Em suma, há razões, derivadas das obras de Strange, que indicam que o fenômeno da difusão de poder operacionaliza-se, ou melhor, difunde-se por meio destas três dimensões, "autoridade", "controle" e "resultados". Durante o processo de operacionalização, estas dimensões culminaram em três variáveis quantitativas ordinais que se encontram presentes no banco de dados, elaborado a partir de artigos jornalísticos, sobre o qual ocorre nossa análise de difusão de poder.

Esta metodologia está estruturada da seguinte forma: iremos expor as três variáveis utilizadas para a análise de difusão de poder, explicar sua operacionalização e escopo de atuação. Na sequência, abordaremos como foi realizada a seleção dos artigos jornalísticos que compõem o banco de dados desta pesquisa. Finalmente, identificaremos os atores oriundos do conjunto de artigos, o banco de dados desta pesquisa e detalharemos o processo que conduziu a análise do fenômeno da difusão em três dimensões a partir dos artigos jornalísticos.

A variável independente é a "Tor Network" e a variável dependente é "difusão de poder". A hipótese é que o uso da rede TOR potencializa a difusão de poder no domínio cibernético. A nossa pesquisa se concentrará em "como" isso é possível e "em que medida" essa difusão de poder ocorre.

16 Dizemos que pode indicar ausência de poder porque nem sempre isto é verdade. A negação do acesso a informação, por exemplo, indica poder por parte do ator que nega. É o que Strange (1988) lembrou que ficou conhecido na literatura como "negarchy", o poder que advém da resistência da alteração de status-quo. Um exemplo clássico o sistema de "pesos e contrapesos" sobre o qual funciona os três poderes, legislativo, executivo e judiciário. A negação de um dos três poderes sobre a influência excessiva de um deles sobre os resultados é indicativo de seu poder. Outro exemplo advém desta pesquisa. Uma das conclusões de nossa análise indica que o ator Tor Project exerce poder quando é capaz de resistir à vigilância digital sobre os usuários e mensagens da rede anônima TOR. Este exercício de poder, apesar de incidir sobre os resultados (a vigilância não ocorre), não altera o status-quo porque o status-quo é a ausência de vigilância. A alteração do status-quo resulta em um cenário diferente em que a vigilância digital, de fato, ocorre.

1.4.1 As variáveis “autoridade”, “controle” e “resultados”

É sabido que Strange (1996), ao discorrer sobre a difusão de poder, não utilizou variáveis que pudessem atestar o fenômeno estudado. Sua metodologia, identificada por ela própria como “funcionalista”, examina as várias funções da autoridade na economia política e realiza questionamentos sobre “quem”, ou “o que”, estaria exercendo estas funções ou responsabilidades – e ainda, com quais efeitos sobre os resultados. (STRANGE, 1996, p.42). Apesar de não ter abordado o fenômeno pela ótica da operacionalização, nós acreditamos que a construção de variáveis quantitativas ordinais seja uma importante tentativa de auxílio na interpretação do fenômeno. Estas variáveis podem, ao menos, balizar o nosso direcionamento analítico em relação a difusão de poder.

Baseado na leitura da obra, a compreensão sobre a difusão de poder é a seguinte: a difusão de poder ocorre quando um ator possui autoridade suficiente dentro de uma estrutura primária, no nível local ou global, de modo a controlar algo que seja capaz de afetar os resultados. Ou seja, o seu controle sobre algo é determinante para os resultados serem da forma que são.[17] De acordo com Strange (1996), a difusão de poder é capaz de explicar o ganho de poder dos mercados frente ao Estado-nação – ou melhor, o ganho de poder de atores não-estatais que atuam dentro de cada uma das estruturas primárias, e por vezes na intersecção entre elas (estruturas secundárias). Sua abordagem atesta a relevância e a força dos atores não-estatais no SI e apontam a urgência em trata-los no âmbito acadêmico afim de realizar pesquisas que possam compreender a prática internacional. Por esta razão, ela distancia-se da disciplina de RI – quase exclusivamente preocupada apenas com o ator Estado – e inaugura a EPI, que abrange os atores não-estatais que atuam de modo transnacional na economia política global.

A tabela descrita abaixo apresenta de forma sistemática as três variáveis adotadas por esta pesquisa (primeira coluna), seu escopo de atuação (segunda coluna) e valores plausíveis (terceira coluna).

17 Ela aponta, por exemplo, que o Estados detém o controle das Forças Armadas que, por vezes, agem de modo a influenciar os resultados para que as preferências do Estado tenha precedência sobre as demais. O controle sobre as Forças Armadas (e outras estruturas) fundamenta a autoridade máxima do Estado dentro da estrutura de segurança. E apesar do Estado encontrar rivais (por exemplo, o crime organizado – que por vezes é conhecido como “o estado paralelo”) dentro da estrutura da segurança, ele ainda mantém-se nesta estrutura como autoridade líder. (STRANGE, 1988).

TABELA 1 - VARIÁVEIS DA DIFUSÃO DE PODER

VARIÁVEIS	ESCOPO DE ATUAÇÃO	VALORAÇÕES		
AUTORIDADE	Confiança dos pares e interessados.	Decrescimento -1	Estabilidade 0	Crescimento 1
CONTROLE	Exerício/operação de objeto.	Nenhum 0	Parcial 1	Absoluto 2
RESULTADOS	Incidência sobre o status-quo.	Não-alteração 0	Alteração 1	

Fonte: Autora.

A primeira coluna, "variáveis", identifica as três variáveis do fenômeno de difusão de poder: autoridade, controle e resultados.[18] A segunda coluna, "escopo de atuação", apresenta o sentido, a ideia por trás de cada variável. Ou seja, apresenta o capo de atuação da variável. A terceira coluna, "valorações", representa por meio de valores máximos e mínimos todas as possibilidades compreendida por cada variável. Exemplo: a variável "autoridade" tem como escopo de atuação a confiança dos pares e interessados. Esta confiança pode decrescer, manter-se estável, ou crescer. Caso verifique-se decrescimento, mediante leitura do artigo jornalístico, a variável "autoridade" receberá o valor "-1". E assim sucessivamente. As valorações de cada dimensão são baseadas na leitura das obras de Susan Strange. Por meio delas, verificou-se que nas situações em que a própria cita o elemento autoridade, por diversas vezes ela analisa, por exemplo, que determinada autoridade encontra-se em declínio, crescimento, ou estabilidade. Em outros momentos, Strange (1988) indica a relevância do controle de objetos capazes de impactar os resultados. E em diversas ocasiões ela salienta a importância dos resultados para a determinação da autoridade, controle e poder de um ator. O fundamento que sustenta a existência das variáveis, escopo de atuação e valorações apresentados nesta tabela é exposto no capítulo um desta pesquisa e respaldam-se na literatura de Susan Strange.

18 Estas variáveis são representativas das dimensões da difusão de poder. Por sua vez, estas dimensões têm origem nas obras de Strange (1988, 1996) que servem de marco teórico desta dissertação. Os termos originais, em língua inglesa, são "authority", "control" e "outcomes", respectivamente.

A primeira variável, "autoridade", refere-se ao sentido da confiança dos pares e interessados.[19] Podemos dizer que algo, ou alguém, possui autoridade suficiente dentro de uma estrutura quando seus pares lhe outorgam confiança, seja de modo formal ou informal. Ou seja, antes de tudo, precisamos identificar o agente/ator em questão como uma autoridade local ou global dentro de, pelo menos, uma das quatro estruturas primárias identificadas por Strange (1988). Caso isto seja possível, segue a sequência explicativa da variável. Caso contrário, não podemos associar o ator à variável "autoridade". Vejamos um exemplo.

Um dentista tem autoridade sobre assuntos dentários, pois o seu conselho de classe lhe conferiu esta outorga por meio de membresia. Ele também tem autoridade sobre estes assuntos porque a faculdade pela qual se graduou conferiu-lhe um diploma de bacharel que lhe permite gozar de determinadas prerrogativas legais – inclusive esta autoridade. Um narcotraficante tem autoridade sobre transações de drogas em uma região porque seus pares, outros narcotraficantes, ou interessados, consumidores do produto, lhe outorgaram essa confiança. Enquanto o dentista é uma autoridade formal, o narcotraficante é uma autoridade informal. Esta "autoridade" pode aumentar (no caso de um dentista isto acontece quando ele pesquisa profundamente assuntos da área, tornando-se especialista em um assunto específico); diminuir (quando este mesmo dentista comete erros graves no exercício da profissão e ele será menos procurado, uma vez que a confiança no seu trabalho diminuirá; caso seja constatada a gravidade do erro, ele pode ser expulso do conselho de classe e ter suas prerrogativas legais suspensas); ou permanecer estável (quando este dentista não se torna especialista em nenhum assunto específico, mas também não comete erros no exercício da profissão – ou seja, ele apenas mantém seu nível de autoridade estável no exercício de suas atividades profissionais).

Um ator tem poder quando ele possui autoridade sobre algo. Esta autoridade pode ter sido outorgada por meios formais ou informais. Vejamos dois exemplos sobre isso. Para ilustrar a formalidade, daremos o exemplo da soberania no SI. A soberania é um poder exercido no SI pois é reconhecido formalmente pelos atores que o compõem, ou melhor, pelos pares do Estado (atores estatais) e interessados (atores não-estatais). Em relação a informalidade, vejamos o exemplo do narcotraficante de uma região. A população local lhe confere autoridade

19 Strange (1988) utiliza o termo "reliability".

por crença comunitária, seja porque ele provê segurança como troca por poder comercializar seus produtos, seja porque ele é demasiado violento na região e a comunidade subordina-se a ele por medo de retaliação. Da mesma forma, o dólar americano é uma moeda com poder que excede as fronteiras estadunidenses pois os demais Estados lhe conferem, informalmente, autoridade quando utilizam esta moeda em suas transações comerciais e financeiras.

Quando a variável "autoridade" aumenta designamos o valor de "+1"; quando diminui designamos o valor de "-1"; e quando permanece estável designamos o valor de "0", pois não há alteração. Esta variável, portanto, pode receber valores inteiros que variam do "-1" ao "+1" (incluso o algarismo "zero") – a depender somente do contexto da situação em que se encontra a autoridade em questão e a análise que se faz a partir deste contexto.

A segunda variável, "controle", refere-se ao sentido do exercício ou operação de um determinado objeto relevante na conquista de influência do resultado. Novamente, precisamos, antes de tudo, identificar se o agente detém o controle sobre o objeto em questão. Caso seja possível averiguar isso, segue a sequência explicativa da variável. Caso contrário, não podemos atribuir a variável "controle" ao agente.

Um ator tem poder quando ele tem o controle sobre algo relevante para o alcance dos resultados por ele desejados. Este poder é a capacidade de alteração do status-quo. Ele pode não ser uma autoridade formal, ou informal, porém, se ele tem a capacidade de controlar este objeto relevante então ele possui poder sobre os resultados. Este seria o caso, por exemplo, de um piloto aéreo militar no comando de uma aeronave bélica. Ele não possui autoridade; ele é instrumento de operação das Forças Armadas a que subordina-se. No entanto, quando, ao sobrevoar uma região, lhe é ordenado que dispare as bombas armazenadas na aeronave, este piloto tem a escolha de lançar as bombas ou não. Naquele momento, ele tem o controle sobre objeto relevante para influência dos resultados: as bombas. Durante este período, este soldado tem poder. Suas ações podem alterar o status-quo (não lançamento da bomba) caso ele deseje.

Algo, ou alguém, apenas controla o objeto se ele exerce, opera, ações para este fim – seja de modo direto (ele próprio) ou indireto (uso de outra pessoa ou mecanismo). A variável "controle", quando presente, determina o grau de operação sobre o objeto: nenhum, parcial ou absoluto. Quando esta variável não pode ser atribuída ao agente em questão, dizemos que o agente não possui controle sobre determinado

objeto e designamos a valoração de "nenhum", que corresponde a "0" visto que seu controle é inexistente. Se o agente possui controle parcial, receberá o valor de "+1". E caso tenha o controle absoluto, será designado o valor de "+2". Esta variável, portanto, pode receber valores inteiros que variam do "0" ao "+2" – a depender somente do grau de controle do agente em questão.

A terceira, e última variável, "resultados", tem como conteúdo o sentido de "incidência sobre o status-quo". E, quando se trata do domínio cibernético, é relevante ponderar sobre os "efeitos sobre a realidade" – que é o domínio no qual encontram-se os atores. Os resultados relevantes são aqueles que incidem no plano real geográfico – e não na virtualidade do campo cibernético. Ora, um resultado apenas tem sentido se ele afeta qualquer aspecto da realidade na qual os atores estão inseridos. Qualquer resultado no plano cibernético apenas será levado em consideração se este resultado incidir, também, no plano real geográfico. Um jogo virtual para lazer pode ter diferentes resultados para os jogadores envolvidos. O jogador A pode ficar na primeira colocação, por exemplo. Mas este resultado não tem nenhuma incidência no plano real geográfico, uma vez que é jogado por prazer. Se, por acaso, o jogo acontecesse dentro do contexto de um campeonato nacional, certamente o primeiro lugar teria alguma incidência no plano real do jogador A: uma compensação monetária, algum prêmio ou título.

Um ator também pode ter poder quando suas ações, com efeitos no plano real geográfico onde os demais atores estão inseridos, alteram ou reforçam o status-quo.[20] É o caso de um jogador de jogos virtuais dentro de um campeonato. Quando ele disputa um jogo contra o campeão mundial, ele não tem autoridade e nem controle sobre o jogo. No entanto, quando ele altera o resultado (ganhando do jogador mundial, por exemplo) ele adquire poder (agora, ele próprio é o campeão mundial). Não alterar o resultado (o campeão mundial continua sendo o campeão mundial), ou seja, reforçar o status-quo, também é uma forma de fazer o seu oponente manter o poder que já possuía.

A variável "resultados" pode indicar alteração do status-quo, ou pode indicar sua não-alteração. Caso indique alteração, designamos o valor "+1" pois o status-quo foi alterado. Caso não indique alteração, designamos o valor "0" pois o status-quo não foi alterado. Esta variável, portanto, pode receber valores inteiros que variam do "0" ao "+1"

20 Como mencionado anteriormente, o poder que deriva do reforço do status-quo está relacionado com a ideia de "negarchy", ou a força que deriva da negação da alteração do status-quo. Strange (1996) pondera sobre a "negarchy" em sua obra.

(incluso o "zero", evidentemente) – a depender somente da análise da alteração do status-quo em questão.

Faz-se necessário apontar que nossa compreensão sobre a operacionalização do fenômeno de difusão de poder não trata sobre ganho, estabilidade ou perda de **poder absoluto**, mas sim de **nível de poder**. São coisas diferentes. Quando um ator tem perda do nível de poder, ele perde *algum* poder. Ele não perde, necessariamente, *todo* o poder. Mas para perder *algum* poder, ele precisa ter *algum* poder. É por este motivo que a situação de não ter *nenhum* poder e, ainda, perder nível de poder não pode acontecer. Não há poder negativo. Agora, se um ator tem estabilidade do nível de poder, isso significa que não há ganho, nem perda, de *algum* poder. O ator, simplesmente, manteve-se no mesmo nível de poder que detinha. Se ele não tinha nada de poder, ele se mantém com nada. Se ele tinha algum poder, manteve-se com esta mesma "quantia" de poder. Seu nível, onde quer que esteja, não é alterado. Finalmente, se há ganho do nível de poder, isto indica que o ator ganhou, necessariamente, *algum* poder. Se ele nada tinha, agora tem *alguma* coisa. Se ele já tinha *alguma* coisa, agora ele tem ainda mais – seu poder é reforçado, reconfirmado.

Finalmente, necessitamos apontar duas observações em relação à operacionalização do conceito adotada nesta pesquisa. Primeiro, nós não propomos que esta operacionalização, juntamente com as variáveis, seja guia definitivo sobre difusão de poder. Mas nós acreditamos que ela pode servir de apoio a uma análise perceptiva sobre ganho, perda ou estabilidade do poder no SI, segundo abordagem da EPI. A ideia central desta operacionalização é acompanhar os artigos jornalísticos selecionados nesta pesquisa cujas ações dos atores são realizadas via rede anônima TOR. Esperamos que esta operacionalização auxilie na análise de cada agente: se estão perdendo, ganhando, ou permanecendo com o mesmo nível de poder. Cada caso só pode ser avaliado individualmente e deve-se respeitar o seu contexto. A atribuição de valores para as variáveis permite, por exemplo, análises estatísticas de correlação que, apesar de não serem utilizadas nesta pesquisa, fornecem insumos para diversas análises. E estamos conscientes de que a operacionalização do fenômeno não deve ser um guia rígido sobre o assunto. Segundo ponto, a atribuição dos valores para cada ator será mediante percepção – uma característica subjetiva. Cada ator, oriundo dos artigos jornalísticos, será analisado por meio das variáveis aqui discutidas de modo a balizar a percepção acerca da difusão de poder no

contexto da rede TOR. Os atores, que compõem a base de dados desta dissertação, serão identificados e discutidos na próxima seção.

1.4.2 A seleção das notícias e composição do banco de dados

A busca por insumos de análise tem cunho investigativo documental uma vez que foi realizada em documentos conservados no interior de órgãos privados jornalísticos. De acordo com Gill (1991), esse tipo de pesquisa tem vantagens por ser considerada uma "fonte rica e estável de dados" por não implicar altos custos e nem exigir contato com os sujeitos da pesquisa. Pádua (1997, p.62) argumenta ainda que a pesquisa documental é a pesquisa que se realiza a partir de documentos contemporâneos ou retrospectivos, considerados cientificamente autênticos (não fraudados) e tem sido utilizada com frequência nas ciências sociais.

Utilizamos a mídia alternativa – mais precisamente os jornais online – para compor o cenário da realidade sobre a qual foi feita a análise de difusão de poder. Riffe, Lacy e Fico (2008) realizam considerações acerca da pesquisa em mídia e apontam que o método científico que corresponde ao "the systematic assignment of communication contente to categories according to rules, and the analysis of relationships involving those categories using statistical methods" é chamado de análise quantitativa de conteúdo. Este método de pesquisa envolve uma série de técnicas que compreendem o exame teórico de literatura e o desenvolvimento de códigos representativos de categorias – cujo objetivo é refletir as diferenças entre os conteúdos. A sua aplicação em conteúdo exposto em comunicações de massa, como os jornais, parte do princípio inicial de que o pesquisador em questão busca levantar uma abordagem, baseada nas ciências sociais, através de observações empíricas e mensurações. Ou seja, há suspeita suficiente para investigar "traços teóricos" em um contexto prático determinado e, assim, propor explicações ou relações entre diferentes conceitos. (RIFFE; LACY; FICO, 2008). Sobre isso, Riffe, Lacy e Fico (2008) confere um exemplo

> 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)

A presente pesquisa envolve a operacionalização de conceitos e análise empírica por meio da investigação documental de artigos jornalísticos e mensurações categóricas – e, portanto, utiliza-se do método cientifico de análise quantitativa de conteúdo como exposto pelos autores supracitados.

Nossa investigação se limitou a dez jornais online de língua inglesa de maior número de visita única por usuário – como exposto na seção justificativa. (COMSCORE, 2012).

TABELA 2 - OS DEZ MAIORES JORNAIS DO MUNDO EM NÚMERO DE CLIQUES POR USUÁRIO (EM MILHÕES)

Posição	País	Jornal	Endereço URL	Nº Visitantes Únicos/Mês
1º	Inglaterra	Mail Online	http://www.dailymail.co.uk	50,067
2º	EUA	The NY Times	https://www.nytimes.com	48,695
3º	Inglaterra	The Guardian	https://www.theguardian.com	38,931
4º	India	Tribune Newspapers	http://www.tribuneindia.com/	35,862
5º	China	People's Daily Online	http://en.people.cn/	33,026
6º	Inglaterra	Telegraph Media Group	https://www.telegraph.co.uk/	30,083
7º	China	Xinhua News Agency*	http://www.xinhuanet.com/english/	29,987
8º	EUA	Washingtonpost.com	https://www.washingtonpost.com/	26,007
9º	EUA	Hearst Newspapers	http://www.hearst.com/newspapers	24,174
10º	EUA	Advance Digital	(conjunto de jornais disposto abaixo)	22,340
		Alabama Local News	http://www.al.com/	
		Cleveland OH	http://www.cleveland.com/	
		Mississippi & Gulf	http://www.gulflive.com/	

Coast	
Le High Valley	http://www.lehighvalleylive.com/
Mardi Gras	http://www.mardigras.com/
Massachussets Local News	http://www.masslive.com/
Michigan Local News	http://www.mlive.com/
New Jersey Local News	http://www.nj.com/
New Orleans, LA Local News	http://www.nola.com/
Oregon Local News Central	http://www.oregonlive.com/
Pennsylvania Local News	http://www.pennlive.com/
Staten Island NY Local News	http://www.silive.com/
Syracuse NY Local News	http://www.syracuse.com/

Fonte: comScore MMX, Worldwide, Age 15+, Oct 2012
*Agência Chinesa de Notícias

O jornal britânico Mail Online é o mais acessado por usuários ao redor do mundo, seguido de perto pelo norte-americano "The New York Times" e, novamente um jornal britânico, "The Guardian". Dois jornais chineses ("People's Daily Online" e "Xinhua News Agency") e um jornal indiano ("Tribune Newspaper") figuram entre os dez maiores jornais em número de cliques por usuário no mundo – embora a lista seja dominada por jornais ocidentais.[21] No relatório da ComScore (2012), o jornal "Advance Digital" é listado na última posição. Apesar de ser listado como um jornal, ele compreende um aglomerado de treze

21 Não foi possível obter quaisquer resultados para o código "Tor Network" no jornal "Xinhua News Agency", agência oficial de notícias do governo chinês. A busca retornava alguns problemas de visualização da página, aparentando entrar em "loop" – quando o usuário faz requisitação para acessar o servidor sem sucesso e o procedimento se repete indefinidas vezes.

jornais norte-americanos. No total, a listagem dos dez maiores jornais do mundo em número de cliques por usuário, elaborada pela Comscore (2012), é composta por 22 jornais com endereços de URL ativos.

Para compor o banco de dados para esta pesquisa, nós visitamos a seção de "arquivos" (base de dados disponível para acesso) de cada um dos jornais listados e realizamos a busca pela expressão "tor network" (com aspas). Com exceção da agência de notícias oficiais da China ("Xhinua News Agency"), os demais jornais trouxeram uma listagem de resultados para a busca.[22] No total, 302 artigos de jornais surgiram como resultados para a busca do termo "tor network". Destes, apenas 195 tratavam da rede anônima TOR – dos quais, 190 eram artigos originais e 5 repetidos. [23] Em suma, do total de 302 artigos de jornais iniciais, apenas 125 tratavam simultaneamente de temas relacionados à estrutura do conhecimento.

Assim, nós buscamos atores não-estatais que tivessem algum grau de reconhecimento social sobre a posse de informações e/ou conhecimento (por definição, Strange não realiza diferenciação entre os dois termos), que fossem responsáveis, de alguma forma, pelo armazenamento de informações, ou que controlassem o canal por meio dos quais estas informações eram comunicadas. Dentro do universo de 190 artigos originais relacionados a rede anônima TOR provenientes dos dez maiores jornais em número de cliques por usuários no mundo, nós averiguamos que 125 artigos abordavam atores não-estatais que satisfaziam as definições acima mencionadas. Em alguns artigos, mais de um ator não-estatal era abordado – de modo que nós optamos por chamar de "ocorrências" as situações envolvendo um único ator não-estatal, e "artigo" as notícias jornalísticas que poderiam versar sobre um, ou mais, ator. Em 14 artigos, nós identificamos dois atores. Cada ator foi tratado como uma ocorrência única merecida de análise.[24] No total, nós identificamos 139 ocorrências passíveis de análise – e estas tornaram-se as 139 linhas do banco de dados desta presente pesquisa. Em outras palavras, isto significa que cada linha do banco de dados representa uma

22Em vez de trazer resultados para a busca do termo citado, o jornal "Xinhua News Agency" buscava o acesso ao servidor repetidas vezes mas sem apresentar a página de resultados. Por esta razão, não foi possível identificar o número de resultados para a busca pelo termo "tor network" nos arquivos de notícias.

23A busca, que foi utilizada definitivamente na pesquisa foi realizada na segunda quinzena de fevereiro de 2018. A primeira busca foi realizada em maio de 2017.

24 Portanto, o foco da nossa pesquisa recaiu sobre o número de ocorrências – e não o número de artigos. Para informações detalhadas, verificar "Apêndice 8 – Artigos e Ocorrências para Análise por Ano".

única ocorrência que compreende apenas um ator não-estatal posicionado dentro da estrutura do conhecimento. Por meio dos artigos jornalísticos, observamos que estes atores realizavam determinadas ações via rede anônima TOR.

TABELA 3 - QUANTIDADE DE OCORRÊNCIAS PARA ANÁLISE (2007-2017)

Ocorrências*	**N**
Resultados para "Tor Network"	302
Conteúdo não-Relacionado a "Tor Network"	105
Conteúdo Relacionado a "Tor Network"	195
Originais	190
Ações via Outros	15
Ações via Tor Network	177
Conteúdo não-Relacionado a Estrutura do Conhecimento	52
Conteúdo Relacionado a Estrutura do Conhecimento*	**125**
Conteúdo 2 atores/artigo	**14**
Conteúdo 1 ator/artigo	**111**
Repetidos	5
Total	**111+(14+14)=139**

Fonte: Autora.
*Situações extraídas dos artigos de jornal composta por um único ator.

**Abrange os artigos compostos por atores que fazem parte da estrutura do conhecimento.

Definida por Strange (1988), a estrutura do conhecimento compreende a crença, o conhecimento estabelecido e os canais de comunicação através dos quais crenças, conhecimento e informações são comunicados. Estes são os três aspectos da estrutura do conhecimento. Esta estrutura também determina que conhecimento é descoberto, o modo como é armazenado e quem comunica este conhecimento – utilizando quais meios, para quem e sob quais condições. (STRANGE, 1988). A rede anônima TOR é um canal de comunicação por meio dos quais crenças, conhecimento e informações são comunicados de forma

segura. Além disso, os atores oriundos dos 125 estão inseridos na estrutura do conhecimento porque realizam ações vinculadas com a descoberta, o armazenamento e a comunicação de informações e conhecimentos por meio da rede TOR. Segundo Strange (1988), os atores posicionados dentro da estrutura do conhecimento ocupam posições relacionadas a tomada-de-decisão. Sobre isto, ela pondera

> [...] 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 acknowledgement 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).

Os atores da estrutura do conhecimento têm a capacidade de afetar os resultados por meio do poder estrutural que, dentro desta estrutura, age de modo menos coercivo e mais baseado no consentimento. De posse deste recorte – artigos jornalísticos relacionados a rede anônima TOR e atores posicionados na estrutura do conhecimento – tivemos a seleção de ocorrências por meio do qual confeccionamos o banco de dados. É a partir deste banco de dados que analisamos a difusão de poder em três dimensões: "autoridade", "controle" e "resultados".

A coluna "COUNTRY" dispõe o nome do país de residência do jornal em questão; "NEWSPAPER", nome do jornal online; "ARTICLE TITLE", título do artigo examinado; "AUTHOR", nome do autor (ou editor) do artigo de jornal; "YEAR", mês e ano de publicação do artigo na mídia jornalística; "ACTOR", ator ou sujeito derivado do artigo de jornal e a partir do qual se examinam as variáveis; "CATEGORY", o grupo temático no qual está inserido o sujeito; "PEERS", os pares e interessados do ator em questão; "AUTHORITY", grau de autoridade do sujeito no artigo de jornal em questão[25]; "OBJECT", o objeto controlado pelo ator segundo o artigo de jornal em questão; "CONTROL", o grau

25 Os graus de autoridade são: crescente, estável, decrescente. Os valores correspondentes são: "+1", "0", "-1".

de controle do objeto pelo sujeito no artigo de jornal em questão[26]; "STATUS-QUO", exposição do status-quo antes da intervenção do sujeito; "EFFECT ON REALITY", se as ações do sujeito no artigo de jornal em questão tiveram efeitos na realidade; "OUTCOMES", o grau de alteração do status-quo, no plano real, pelo sujeito no artigo de jornal em questão[27].

26 O grau de controle pode varia entrar "nenhum", "parcial" e "total" cujos valores correspondentes são "0", "1" e "2".

27 O grau dos resultados varia entre "alteração" e "não-alteração" do status-quo. Os valores correspondentes são "+1" e "0".

QUADRO 2 - AS COLUNAS DO BANCO DE DADOS DESTA PESQUISA

Coluna	Informação
COUNTRY	País de localização do jornal.
NEWSPAPER	Nome do jornal responsável pelo artigo.
ARTICLE TITLE	Título do artigo.
AUTHOR	Autor do artigo.
YEAR	Ano de publicação do artigo.
ACTOR	Ator cujas ações são descritas no artigo.
CATEGORY	Grupo temático da ocorrência.
PEERS	Identificação dos pares e interessados.
AUTHORITY	Identificação da variável "AUTORIDADE" na ocorrência. Recebe os valores: "-1" para designar autoridade decrescente, "0" para designar autoridade estável e "+1" para designar autoridade crescente.
OBJECT	Objeto de controle do ator identificado na ocorrência.
CONTROL	Identificação da variável "CONTROLE" na ocorrência. Recebe os valores: "0" para designar controle nenhum, "1" para designar controle parcial e "2" para designar controle absoluto.
STATUS-QUO	Apresenta o status-quo da ocorrência.
EFFECT ON REALITY	Identifica se as ações do ator têm efeito na realidade. Em caso positivo, atribue-se a expressão "YES". Caso negativo, atribue-se "NO".
OUTCOMES	Identificação da variável "RESULTADOS" na ocorrência. Recebe os valores "0" para designar não-alteração do status-quo e "1" para designar a alteração do status-quo.
REPEATED ARTICLES	"SIM" para indicar que o artigo do qual extraiu-se a ocorrência está presente em outra linha do banco de dados e "NÃO" para indicar a originalidade do artigo.

Fonte: Autora.

A coluna "CATEGORY" foi estipulada por nós e formulada de modo a compreender os atores em grupos de temas similares segundo a

leitura dos artigos jornalísticos. São seis categorias: Digital Security, envolve temas referents à segurança digital; Surveillance Circunvention refere-se a temas relacionados com blindagem contra a vigilância digital; Journalism & Whistleblowing relaciona-se com temas da profissão de jornalismo e denúncias por fontes; Online Marketplace, os mercados digitais que operam na rede anônima; Privacy, envolvem notícias que versam especificamente com dados dos usuários. No total, identificamos a existência de 25 atores não-estatais, os quais compreendemos nas seis categorias supracitadas: Digital Security – Dan Egerstad, Iranian Cyber Army, Freedom Hosting, Onion Ransomware, SimpleLocker Android Malware, Ransomware; Surveillance Circunvention – Tor Project e 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.

A partir do artigo de jornal pôde-se extrair as informações necessárias para preencher o banco de dados. Além da criação das categorias, compostas por atores com temas similares, identificamos também quem são os pares e interessados nas ações e atividades do ator em questão. Esta coluna "PEERS" têm o objetivo de identificar quem são os sujeitos cujo grau de confiança em relação ao ator aumenta, diminui ou mantém-se estável. Como vimos, este grau de confiança é traduzido pela variável "autoridade" – por isto a coluna "PEERS" foi criada, ou seja, para fornecer fundamento à variável "autoridade". Além desta coluna, também identificamos quem são os objetos relevantes para o alcance dos resultados, pretendidos pelo ator em questão, através da coluna "OBJECT". O grau de controle sobre o objeto exposto nesta coluna traduz-se na variável "controle". Por esta razão houve necessidade de identificar o objeto de controle. A coluna "STATUS-QUO" busca identificar o estado da situação anterior às ações do sujeito porque é a partir da alteração, ou manutenção, deste estado que atribui-se valores à variável "resultados". Mas, antes de atribuir este valor, precisamos saber se a alteração, ou manutenção, do status-quo incide sobre a realidade geográfica pois esta pesquisa atua dentro do ciberespaço. Caso tenha efeito sobre a realidade, atribui-se o valor coerente com a mudança, ou manutenção, do status-quo. Caso não haja efeito sobre a realidade, atribui-se o valor "zero". Novamente, o preenchimento destes campos são realizados a partir do conteúdo dos artigos de jornal.

De modo resumido, a metodologia utilizada nesta pesquisa utiliza as abordagens qualitativas e quantitativas para efetivar a análise dos objetivos específicos. A abordagem qualitativa se dá pelo exame da revisão de literatura, preparação e transcrição do banco de dados a partir das fontes de jornais online alternativos, pré-análise com leituras flutuantes, categorização e apresentação de resultados. A abordagem quantitativa, por outro lado, preocupou-se com atribuição de valoração numérica de modo a auxiliar na interpretação da difusão de poder em cada dimensão sobre o conjunto de artigos jornalísticos selecionados. De modo geral, os componentes do método foram: a inclusão de jornais online para estruturação do banco de dados; a delimitação da estrutura do conhecimento – por meio da qual excluiu-se a análise das demais estruturas apresentadas por Strange (1988); a definição das variáveis e possíveis valores atribuídos às mesmas; o período e a forma da coleta de dados que compuseram o banco de dados. Quanto a análise de dados dentro da abordagem quantitativa, os mesmos estão expostos em tabelas, quadros, gráficos e estatística descritiva – a partir do cálculo de frequência e porcentagem relativa. O recurso utilizado foram planilhas e cálculos no Microsoft Excel 2010. A análise dos dados foi realizada por tabulação de variáveis através da estatística descritiva – com frequência absoluta e relativa simples. A partir deste método realizamos considerações sobre o fenômeno de difusão de poder no contexto da rede anônima TOR, componente da Dark Web.

1.4.3 Composição do Banco de Dados da pesquisa

Para fins de compreensão, selecionamos aleatoriamente um artigo de jornal a fim de demonstrar o preenchimento de cada coluna de informação.

O artigo é intitulado *Global Drug Survey findings: more people buying drugs online in the UK*, publicado em 14 de abril de 2014 pelo jornal *The Guardian*, sediado no Reino Unido e cuja autoria é de "Ami Sedghi". O artigo em questão trata do aumento de compras online por drogas no Reino Unido e aborda o ator Silk Road, mercado online que opera na rede anônima TOR. Segundo o artigo, quase 60% dos entrevistados tinham conhecimento do mercado Silk Road, enquanto cerca de 44% afirmaram que já tinham visitado o site. Os pares e interessados são os cidadãos privados. A partir deste artigo em questão,

designamos o valor "+1" (autoridade crescente) para a variável **autoridade** porque mais da metade dos entrevistados demonstravam conhecer o mercado online e o artigo citava que mais pessoas estavam comprando drogas online no Reino Unido. Interpretamos que, para os pares e interessados do mercado, a confiança depositada no mesmo têm crescido. O objeto de controle do ator Silk Road é o próprio mercado online por meio da sua página e seu mecanismo de pagamento em BitCoins. Portanto, para a variável **controle**, nós designamos o valor "+2" (controle absoluto) tendo em vista que o controle tanto das operações do mercado online como do mecanismo de pagamento são administrados/controlados por um único ator – que é o próprio Silk Road. O controle destes objetos não depende e/ou é compartilhado com nenhum outro ator. Nós identificamos que o status-quo da situação abordada pelo artigo de jornal mencionado é a quantidade fixa de pessoas no Reino Unido que consomem drogas através de compras online. O ator Silk Road altera este status-quo na medida que contribui para o aumento do número de pessoas no Reino Unido que compram drogas online. E essa alteração do status-quo tem efeito no plano real porque as pessoas estão, de fato, consumindo entorpecentes e substâncias ilícitas. Para a variável resultados, nós designamos o valor de "1". E, finalmente, o artigo em questão é original – ou seja, um artigo com um único ator. Não existirá outro ator a partir deste mesmo artigo.

Cabe lembrar que, ao designar os valores recebidos pelas variáveis, nós também identificamos os pares e interessados (autoridade), o objeto relevante para o alcance dos resultados desejados (controle) e o status-quo, modo que pudéssemos examinar se houve alteração (resultados). Estas informações encontram-se no banco de dados desta pesquisa disposta integralmente no apêndice da Dissertação.

1.5 ESTRUTURA DA DISSERTAÇÃO

A dissertação encontra-se divida em três capítulos. O primeiro capítulo versa sobre os aportes teóricos, dentro da área de RI, que será utilizado no terceiro capítulo como fonte de interpretação dos resultados obtidos. Buscou-se expor o conteúdo de uma perspectiva ampla em direção a perspectivas específicas.

De modo resumido, a primeira parte do capítulo um orienta o leitor acerca da acadêmica britânica Susan Strange, expoente da área de

RI e EPI: breve biografia e principais contribuições. Na segunda parte, exploramos as naturezas do poder estrutural e do poder segundo duas abordagens clássicas de RI – abordagem relacional e dos elementos nacionais. A exploração das duas abordagens serviu como fundamentação das razões que levaram Strange a adotar, dentro de RI, nova posição acerca do poder. Esta ruptura com o poder segundo abordagens clássicas da disciplina de RI está no cerne de seus estudos. A terceira parte expõe o fenômeno da difusão de poder segundo Strange. A compreensão do fenômeno necessita dos conceitos de poder relacional e poder estrutural, afinal, ele está circunscrito ao quadro analítico estrutural formulado por Strange dentro da EPI. Este quadro analítico compreende o tecido econômico e político sobre os quais subordinam-se pessoas e serviços. Fecharemos o primeiro capítulo com algumas considerações sobre difusão de poder no domínio cibernético que foram realizadas por Nye (2011), no livro *The Future of Power*, com o objetivo de complementar os estudos de Strange (1996), afinal ela não realizou considerações acerca do ciberespaço.

O segundo capítulo versa sobre o aspecto tecnológico dos sistemas de informação. Na primeira parte discutimos, brevemente, a natureza tecnológica e o surgimento da Internet. Na segunda parte, abordamos a WWW, "Surface Web" e "Deep Web". Na terceira, apresentamos as classificações da "Deep Web" que, segundo Sherman e Price (2001), situam a "Dark Web" no contexto da Internet. Finalmente, buscamos explicar, de modo sucinto, os aspectos tecnológicos que tornam a rede online de baixa latência TOR distinta das demais redes que compõem a Dark Web. A natureza desta rede é o ponto de partida das atividades realizadas por diferentes atores nela inseridos, afinal, são as especificidades da rede TOR que possibilitam o surgimento de um conjunto de cenários que não são suportados na web convencional.

O terceiro capítulo apresenta o banco de dados a partir do qual examinaremos a difusão de poder sob o viés das três dimensões, "autoridade", "controle" e "resultados". Esta é a operacionalização do fenômeno de difusão de poder apresentado por Strange (1996). Nesta análise atribuímos as valorações correspondentes a cada variável. A interpretação final ocorrerá através da frequência de valor, de cada variável para cada grupo e ator. Ao final do capítulo, apresentamos brevemente os resultados da análise.

As considerações finais foram realizadas reunindo o aporte teórico, a natureza da tecnologia em questão e o exame do banco de dados segundo a operacionalização do conceito de difusão de poder para

averiguar o fenômeno no domínio cibernético – especificamente no contexto da rede TOR.

1.6 ÚLTIMAS CONSIDERAÇÕES

Tradicionalmente, a área de RI evidenciava duas principais abordagens em relação ao poder – poder relacional e poder material. [28] Foi a reflexão sobre o cenário internacional, a partir de um quadro analítico, que revelou a lacuna sobre o poder dentro da disciplina de RI – uma vez que as abordagens realizavam análises acerca do Estado. Esta visão do Estado como ator principal ou único, para Strange (1996), é demasiadamente restrita porque não corresponde à realidade dos fatos oriundos do SI: por diversas vezes o poder de corporações transnacionais, e outros atores não-estatais, são sentidas e demonstradas no cotidiano de milhões de pessoas embora ignoradas em análises acadêmicas. Segundo ela própria, "what the notion of structural power in world politics, society and economy did was to liberate de study of international political economy from the so-called realist tradition in the study of international relations". (STRANGE, 1996, p.x) E mais: para Strange (1996), a difusão de poder era a explicação adequada para o fato de que a qualidade da autoridade do Estado se encontrava em declínio, ao passo que a autoridade de outros atores encontrava-se em franco crescimento.

Contudo, de acordo Palan (1999), Strange não pode ser resumida dentro de uma dicotomia padrão entre teoria e prática por duas razões: além de não ser teórica, ela não é "empírica". Ou seja, Strange não era uma figura interessada em teoria, mas sim em promover um quadro de análise por meio dos quais os assuntos pudessem ser explorados. Por esta razão, o livro *States and Markets* deixava claro o dilema entre teoria e o ato de "teorizar", além de não evidenciar empiricismo. (PALAN, 1999, p.123). Acreditamos que este dilema também se torna evidente no livro *The Retreat of the State: The Diffusion of Power in the World Economy*, de 1996. Embora apresente temas inovadores, como a profissão contábil e a Máfia no cenário da economia política global, a autora não apresenta nem método e nem evidências empíricas que atestem o fenômeno da difusão de poder – pelo menos de acordo com o rigor acadêmico. Contudo, esta observação não

28 Baldwin (2013) chama estas abordagens de "relacional" e "elementos nacionais de poder", respectivamente.

procura diminuir em nenhum grau o trabalho e a exploração pioneira de Strange acerca do ineditismo da abordagem de EPI. Como sugeriu Palan (1999), talvez tal rigor acadêmico evidenciado pela empiria provocasse nela preocupações quanto ao distanciamento da realidade. E ela deixou em aberto o convite a pesquisadores para apresentar trabalhos teóricos e empíricos acerca do tema das autoridades não-estatais e como elas afetam as quatro estruturas em EPI. Sobre isso, ela afirma que

> 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)

A partir do convite da própria autora, esta dissertação busca explorar estudos acerca da estrutura do conhecimento de modo a examinar autoridades não-estatais e a difusão de poder atuantes no domínio do ciberespaço, especificamente no contexto da rede anônima TOR. Faremos isso de dois modos: primeiro, buscamos explicitar as três dimensões do poder estrutural que, embora não tivessem sido tratadas como dimensões nas obras de Strange, estão contidas em seus escritos; e, segundo, operacionalizamos o conceito de difusão de poder, a partir das três dimensões, de modo a abranger análise empírica. Nosso objetivo é contribuir academicamente para os estudos em EPI.

2. CAPÍTULO 1: MARCO TEÓRICO

O objetivo deste capítulo é apresentar o aporte teórico, dentro da área de Economia Política Internacional (EPI), que será utilizado no terceiro capítulo como insumo para interpretação das análises de difusão de poder no contexto da rede anônima The Onion Router (TOR) publicado por documentos jornalísticos.

Neste primeiro capítulo, partimos de uma perspectiva ampla do conceito tradicional de poder em Relações Internacionais (RI) em direção à apresentação do conceito alternativo de poder elaborado por Strange (1988) chamado por ela de "poder estrutural". Este conceito alternativo é apresentado com especial atenção à estrutura do conhecimento. Esta estruturação visa prover fundamentos suficientes para a explicação do fenômeno de "difusão de poder" – que será apresentado na sequência e compõe o marco teórico desta dissertação. O fenômeno de "difusão de poder" é calcado a partir do poder estrutural.

Na sequência, nós exploramos as três dimensões que, segundo nossa interpretação, são essenciais para a compreensão do fenômeno da difusão de poder: "autoridade", "controle" e "resultados". Estas três dimensões estão presentes na obra de Strange (1988, 1996), embora não houvessem sido explicitadas de tal forma pela autora. Esta seção do capítulo fornecerá os insumos necessários para averiguar a existência da difusão de poder e sua medida no contexto da rede anônima TOR (que faz parte da estrutura do conhecimento) – o que será feito no terceiro capítulo da dissertação.

Finalmente, apresentaremos, de modo breve, o que a literatura de RI sobre poder tem arguido no domínio cibernético – com exploração dos conceitos de "cyber power" e "difusão de poder" de Joseph Nye (2011).

De modo resumido, o primeiro capítulo está disposto segundo os seguintes tópicos temáticos: breve introdução biográfica de Strange; mapeamento das discussões tradicionais de poder em RI – de modo a evidenciar as lacunas teóricas exploradas por Strange, que provocou a ruptura com a literatura de RI e elaborou o quadro analítico estrutural em EPI pelo qual se tornou conhecida; apresentação do poder estrutural e da estrutura do conhecimento; apresentação do fenômeno da difusão de poder; exploração das três dimensões "autoridade", "controle" e "resultados" e suas respectivas conexões com o fenômeno da "difusão de poder"; exploração sobre a literatura atual de poder em RI no domínio cibernético.

2.1 BIOGRAFIA E ATUAÇÕES DE SUSAN STRANGE

Nascida em 1923 e graduada em Economia pela London School of Economics (LSE) em 1943, Susan Strange, considerada por muitos a mais influente figura em estudos internacionais britânicos, foi quase exclusivamente a responsável por criar a área da EPI no século XX. (BROWN, 1999). Ela iniciou a carreira no jornalismo, antes de ingressar nos estudos internacionais. De acordo com Brown (1998) o fato de ter ingressado tardiamente contribuiu para que ela se mantivesse intacta em relação às seduções ao ego, uma vez que a academia é marcada não apenas pelo aprendizado mas por suas instituições e prestígio.

A erudita Strange era uma voz ecoante sobre a fundição de duas grandes disciplinas, a Economia e a Política. Ela acreditava que esta fundição seria capaz de promover o surgimento de um novo campo em RI. Sobre isso, Brown (1999) afirma que existem dois pontos fundamentais para entender as razões que a levavam a advogar a fundição das duas áreas no contexto global: (1) salvo algumas exceções, muitas vezes ela acreditava que ou os economistas deixavam de considerar o papel do poder no cenário global, ou eram demasiadamente confiantes em seus modelos econômicos abstratos e formais sobre o mundo real; (2) a maioria dos cientistas políticos parecia excessivamente impressionada as forças militares e o poderio bélico e, por esta razão, creditavam mais poder às instituições do que elas de fato possuíam. Brown (1999) também não deixa de apontar que a compreensão sobre os trabalhos de Strange deve partir de sua característica mais evidente: o ecleticismo. Esta característica seria a base da interdisciplinariedade da própria disciplina de EPI.[29]

Durante cerca de dez anos, entre 1965-1976, Strange foi pesquisadora integral da Chantham House. É neste período que publica seu manifesto *International Economics and International Relations: A Case of Mutual Neglect*, de 1970, em que advoga a nova abordagem de

29 Alguns de seus trabalhos incluem: “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 – trabalho conjunto a John M. Stopford e John S. Henley”; “The Retreat of the State: The Diffusion of Power in the World Economy”, 1996; “Mad Money: When Markets Outgrow Governments”, 1998.

análise para RI, compreendida pelo amálgama das áreas de Economia e Política, de modo a compreender a realidade das interações e forças no contexto global.[30] (BROWN, 1999).

Seja como for, os esforços de Strange para tornar a área de EPI evidente, e atrair estudiosos interessados em realizar análises conjunturais e sistêmicas, são inegáveis. Quanto a isso, estudiosos apontam que ela gerou algo muito próximo de uma teoria alternativa de RI, embora não tenha sido reconhecida como teórica e nem tenha aceitado ela própria este rótulo. (PALAN, 1999; COHEN, 2016). Seus estudos sobre poder evidenciam a sua abordagem intelectual sobre temas da agenda de RI e Economia. Cohen (2016) aponta que o elemento do poder é central para qualquer explicação do caráter e da dinâmica da economia global. Tooze e May (2002) consideram que as análises de Strange sobre poder formam a mais significativa contribuição para a área de EPI. A erudita Strange configura-se como um dos grandes destaques das disciplinas de RI e EPI.

2.2 O PODER SEGUNDO ABORDAGENS TRADICIONAIS DE RI

As Relações Internacionais inauguraram o campo de estudo cujo domínio pertence ao que convencionou-se designar de "política internacional". (PORTER, 2013, p.4) O cientista político norte-americano Quincy Wright (1955) explicou o termo "política internacional" no sentido de influenciar "major groups in the world so as to advance the purposes of some against the opposition of others." [31] (WRIGHT, 1955).

30 A partir do manifesto, originou-se uma conferência, sob a tutela da Chatham House, que reuniu grupos de acadêmicos de diversas áreas dos EUA e Reino Unido, em 1972. Por sua vez, esta conferência produziu, dois anos mais tarde, a formação da *International Political Economy Group* (IPEG) sob organização de Strange dentro da *British International Studies Association* (BISA), também formada a partir de iniciativas próprias. (BROWN, 1999).

31 Esta explicação tem, como consequência, uma expressiva conotação política que abrange a esfera do internacional. Mas não para dizer que apenas os Estados estão envolvidos em política. Outros sujeitos também são atores relevantes. O filósofo político Bertrand de Jouvenel (1957) sugere que os sujeitos envolvidos em política vão além dos próprios políticos, das pessoas que participam de partidos políticos ou, até mesmo, de movimentos sociais com objetivos explicitamente políticos. Ele ressalta dois pontos fundamentais: primeiro, uma ação se torna política quando a ajuda de outros é uma condição necessária para que um indivíduo alcance seu objetivo; segundo, como consequência, a política

O cientista político na Universidade de Princeton e professor emérito na Universidade de Columbia, Baldwin (2013), acredita que todas as "políticas" são políticas que envolvem o elemento do poder, mesmo que discuta outros elementos. Podemos extrair disto que a política internacional também lida com o elemento do "poder" – tanto a partir do nascimento de RI como disciplina, em 1919, quanto dos estudos realizados em política internacional sobre eventos muito anteriores a isto (como, por exemplo, a Guerra do Peloponeso, amplamente discutida pela disciplina).[32] (HENDEL, 1953; WALTZ, 1979; WALT, 1987; MOUL, 1989; CLAUDE, 1989; GUZZINI, 2000; SCHWELLER, 2006; KAUFMANN, LITTLE, WOHLFORTH, 2007; LITTLE, 2007; BROOKS, WOHLFORTH, 2008).

O elemento "poder" é amplamente relacionado, e frequentemente associado, com a corrente teórica do Realismo, apesar de não ser tratado apenas por ela. Sobre isso, Wendt (1999) comenta que a característica definidora do Realismo, de fato, é a asserção de que a natureza da política internacional é moldada pelas *relações de poder*. Porém, ele também lembra que esta característica não é única ou exclusiva do Realismo.[33]

---

acontece quando um projeto demanda o apoio da vontade do outro. Em RI, a política é tratada, com frequência, como aquela que envolve governantes e membros do alto-escalão do governo de um Estado. Assim, é neste aspecto que Strange difere dessa concepção de política difundida pela área de RI. A britânica parte de premissa similar à de Bertrand De Jouvenel, de que a política não envolve apenas governantes mas todos aqueles que agem a partir da vontade do outro, para realizar considerações acerca da dinâmica política do poder. Por esta razão consegue observa atores não-estatais como sujeitos políticos e os abrange dentro do quadro analítico que formula para compreender a EPI. Atores estatais e não-estatais podem ser vistos à luz deste quadro analítico – o que é diferente das abordagens tradicionais de RI.

32 A disciplina tem quase um século de história. Acredita-se que sua origem foi em 1919, com a criação da primeira cadeira para o estudo de política internacional no mundo—no Departamento de Política Internacional1 da Faculdade Universitária de Gales, "Aberystwyth". (SCHMIDT apud PORTER, 2013). Em 2019, a Universidade de Aberystwyth, como é conhecida, comemorará o centenário da disciplina e já declarou que a fundação do departamento foi uma "[…] resposta a violência extrema da Primeira Guerra Mundial em que milhões de pessoas de vários lugares do mundo perderam suas vidas. Esta fundação constituiu uma resposta intelectual a um evento global com uma finalidade normativa: compreender as diferentes facetas da política mundial (política, direito, economia, ética) de modo a atenuar a violência organizada." (ABERYSTWYTH UNIVERSITY, 2017, tradução nossa). Através das décadas, a disciplina progrediu academicamente promovendo, inclusive, sucessivas ondas de fases teóricas: idealismo, realismo, behavioralista, pós-behavioralista, pluralista, neorealista, racionalista, pós-positivista e construtivista. (SCHMIDT, 2017)

33 De acordo com Baldwin (2013), apesar das discussões sobre "poder" em RI terem tido pouco sucesso em gerar consenso, existe uma concepção básica sobre poder que é a mais amplamente aceita: formulada inicialmente por Dahl (1957), é a ideia de que o ator A

Segundo Baldwin (2013) são duas tradições que dominam os estudos sobre análise de poder em RI: a abordagem dos "elementos nacionais de poder" e a abordagem do "poder relacional". A primeira trata o poder como um recurso. A segunda o identifica como uma relação seja ela existente ou em potencial. Analisaremos estas duas abordagens a seguir de forma a compreender o panorama do estudo sobre poder que antecedeu os estudos de EPI.

2.2.1 Abordagem dos Elementos Nacionais de Poder

A abordagem dos "elementos nacionais de poder" trata o poder em termos de recursos, sendo passível de posse por um ator. Ou seja, estes recursos são tratados como se fossem o próprio "poder" (BALDWIN, 2013, p.277). Não há consenso sobre o que são estes recursos, embora existam interpretações indicando que são os elementos que compõem uma nação e possíveis de quantificar como, por exemplo, tamanho do território, número de habitantes, grau de riqueza, etc. (Ibid., p.280). Esta noção do poder com viés de propriedade está inserida nas correntes teóricas que versam sobre a "balança de poder". (Ibid., p.281). De acordo com Wright (1965), o termo "balança de poder" compreende uma ideia de que as mudanças que decorrem do poder político relacional têm a capacidade de serem observadas e mensuradas na prática: ou seja, o poder é um recurso que pode ser medido. Isto está em acordo com a noção de "posse", "propriedade", domínio – cerne da abordagem dos "elementos nacionais de poder". [34]

São três correntes teóricas que fazem isso: a teoria clássica da balança de poder, de Hans Morgenthau (1948); o neorrealismo, também conhecido como realismo estrutural ou realismo defensivo, de Kenneth Waltz (1979); e o realismo ofensivo, de John Mearsheimer (2001).

Hans Morgenthau é o expoente mais conhecido da **teoria clássica da balança de poder**.[35] Para ele, se quisermos determinar o poder de

causa (ou tem a habilidade de causar) em B uma ação que B não teria sem a intervenção de A. Esta é a concepção do poder relacional.

34 O termo "balança de poder" é amplamente discutido na literatura de RI pois diferentes autores argumentam que a expressão é demasiadamente ampla. (POLLARD, 1923; SHEEHAN, 1996; BALDWIN, 2013). Baldwin (2013) aponta que o próprio Morgenthau admitiu utilizar o termo para dar significado a quatro noções diferentes.

35 Todavia, o conceito é trabalhado desde muito antes do século XX: ele foi utilizado pelo historiador grego Tucídides na tentativa de explicar o início da Guerra do Peloponeso, como reportado por David Hume (1742) em seus ensaios. De qualquer modo, para Michael Sheehan (1996), a noção de "balança de poder" é uma das mais importantes

uma nação, precisamos distinguir os elementos em dois grandes grupos: o grupo dos elementos relativamente estáveis e o grupo dos elementos sujeitos a mudanças constantes. [36] Na perspectiva de Morgenthau (Ibid., p.109), cabe aos responsáveis pela política externa de uma nação, e aos que moldam a opinião pública com respeito aos assuntos internacionais, avaliar corretamente o impacto desses fatores sobre o poder não só de sua própria nação, como também sobre o de outras nações – o que remete à ideia da balança de poder.

Paul (2004, p.4) observa que a teoria da balança de poder é sedimentada na noção de que os Estados buscam dois objetivos: sobreviver de modo independente e acumular poder no sistema anárquico. Sem poder, eles correm o risco de se tornarem submissos à vontade dos demais, perder segurança e prosperidade. Por esta razão, a anarquia é o elemento que incita os Estados a aumentar o seu poder: tanto a segurança quanto a sobrevivência física não podem existir separadas da maximização do poder. Diante deste cenário, nada mais lógico que a existência da competição pelo poder. Estados mais fracos, de acordo com Paul (2004), poderiam perder a sua segurança, ou até mesmo cessar a sua existência, diante da aliança de um grupo de Estados que o ameace. Assim, os atores mais fracos do cenário se reúnem de modo a formar coalizações para equilibrar o poder frente aos atores mais fortes.

Tais observações fazem parte da chamada teoria clássica da balança de poder que, segundo Baldwin (2013), observa a força militar como uma capacidade de conquistar a guerra, visto que é discutida dentro de um quadro analítico que supõe o confronto armado entre os Estados. Por isto, esta teoria tem seu significado atrelado ao contexto militar.

---

ideias na História por dois motivos: primeiro, é um conceito-chave que, para estudiosos das Relações Internacionais, detém a compreensão dos padrões de comportamento recorrentes dos Estados vivendo sob a sombra da anarquia; e, segundo, porque serve como um guia para muitos estadistas.

36 Neste primeiro grupo estão fatores como a geografia e os recursos naturais (como os alimentos e as matérias-primas. No segundo grupo entram a capacidade industrial, o grau de preparação militar (como a tecnologia, a qualidade da liderança, a quantidade e a qualidade das forças armadas), população (distribuição, tendências), características nacionais (certas qualidades do intelecto e caráter), a moral nacional (ou seja, o grau de determinação pelo qual uma nação apoia a política externa de seu governo tanto em tempos de guerra como de paz; entram neste julgo a instabilidade da moral e a qualidade da sociedade e do governo) e a qualidade da diplomacia (observa-se aqui a qualidade do governo, que também foi tratado dentro da moral nacional; o equilíbrio entre os recursos e a política; o equilíbrio entre os recursos; e o apoio popular). (MORGENTHAU, 1948).

Conhecido como **"realismo estrutural"** ou **"realismo defensivo",** o neorrealismo foi desenvolvido por Kenneth Waltz na obra intitulada *Theory of International Politics*, de 1979. Dentre alguns pontos, ele introduz teoricamente a concepção de uma estrutura dentro do SI. Para Waltz (1979), "any approach or theory, if it is rightly termed 'systemic', must show how the systems 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). Esta concepção estrutural é o elemento teórico que diferencia esta corrente da corrente anterior.

O neorrealismo concebe a estrutura política a partir de três asserções: princípio ordenador, que é o modo pelo qual estão organizados ou ordenados; diferenciação das unidades e a especificidade de suas funções; e a distribuição das capacidades entre as unidades.[37] (Id., 1979, p.88) Veja que, apesar da "distribuição das capacidades" ser um elemento fundamental do neorrealismo, Baldwin (2013) aponta que Waltz não define o que são capacidades e, ao mesmo tempo, admite que os Estados possam ser listados, por exemplo, do mais ao menos poderoso segundo a capacidade de cada um. Isto permitiria a interpretação de que as capacidades são os próprios recursos de poder.

O **realismo ofensivo** surge com a obra de John Mearsheimer, *The Tragedy of Great Power Politics*, em 2001. A ideia por trás dessa corrente tem dois *modus operandi*, ambos relacionados com as ações de um Estado frente a balança de poder: ou ele age de modo a defender a balança de poder, ou age de modo a enfraquecê-la.[38] A defesa ou a "sabotagem" da balança de poder relaciona-se com o medo. De acordo com Mearsheimer (2001), o medo é fundamentado em três lógicas: primeiro, a ausência de uma autoridade central supranacional que pudesse ofertar proteção aos Estados, de modo que não descendessem ao

37 Originalmente, o termo utilizado por Waltz (1979) é "capabilities". De acordo com o dicionário Macmillan (2017), "capability" tem dois significados: o primeiro, "the ability to do something" (traduzido por nós como sendo "a habilidade de se fazer algo"); o segundo, "the number of weapons, soldiers etc that a country has for fighting a war" (traduzido por nós como sendo "o número de armas, soldados, etc., que um país possui para lutar na guerra").

38 Primeiro, um Estado poderoso age de modo a defender a balança de poder do qual faz parte quando o risco de uma mudança (no equilíbrio da balança) favorece outro Estado (que não ele próprio). Caso contrário, ele age de modo a enfraquecer a balança de poder – mas isso só acontece quando o risco de mudança favorece a si mesmo. (Ibid., p.3) Além disso, Mearsheimer (Ibid., p.3) oferece uma razão para este comportamento: a estrutura do sistema internacional "força" os Estados, que buscam apenas segurança, a agirem de modo agressivo uns com os outros.

conflito armado; segundo, a existência do poderio bélico, ou melhor dos recursos militares, das capacidades ofensivas dos Estado; terceiro, o fator da incerteza que impera no SI (uma vez que os Estados nunca estão, de fato, seguros sobre as intenções dos demais). Estes três fatores explicam o medo dos Estados no SI anárquico. Como consequência, o Estado acaba assimilando que quanto mais poderoso ele é em relação ao seu rival, mais chances ele possui de sobrevivência. Disso, extrai-se que a melhor estratégia de sobrevivência é tornar-se o "hegemon" do SI porque os Estados não poderiam ameaçar o "hegemon" de modo sério dada a posição de poder dele. (Ibid., p.3)

As três correntes teóricas, da disciplina de Relações Internacionais, supracitadas detém pontos em comum e pontos divergentes.[39] De acordo com Baldwin (2013), muito embora a abordagem "dos elementos nacionais de poder" se faça presente na literatura sobre o assunto, ela apresenta alguns problemas analíticos por apresentar o poder propriamente como um *recurso*. Se o poder é um recurso, e recursos são estáticos, o que funciona como recurso de poder em uma ocasião pode não funcionar em situação diferente – uma vez que o contexto se altera. Além disso, recurso está atrelado ao poder potencial, diferente do poder *de fato.* (BALDWIN, 2013).

Deste modo, percebe-se que a característica fundamental da perspectiva dos "elementos nacionais de poder" é o entendimento de que o poder pode ser mensurado pelos recursos de um Estado. Além disso, pressupõe-se que os Estados saibam traduzir o poder oriundo dos recursos em objetivos nacionais definidos.[40] (SHEEHAN, 1996)

---

39 Tanto Hans Morgenthau e Kenneth Waltz quanto John Mearsheimer1 observam o poder a partir de uma perspectiva essencialmente militar. (BALDWIN, 2013, p.283). O realismo clássico e o realismo ofensivo apresentam os Estados como atores que buscam maximizar o poder. Mas, enquanto que para Morgenthau (1948) a explicação disso reside no desejo pelo poder em si, para Mearsheimer (2001) a maximização de poder é uma consequência natural oriunda do sistema internacional, essencialmente anárquico, dentro dos quais os Estados residem. (BALDWIN, 2013, p.283) O realismo defensivo e o realismo ofensivo retratam os objetivos dos Estados como sendo derivados da estrutura do sistema internacional. No entanto, Waltz (1979) define que o objetivo é manter para si uma porção de segurança suficiente de modo a garantir a sobrevivência do Estado. Não há razão para reunir mais poder do que o necessário para sua sobrevivência. Enquanto isso, Mearsheimer (2001) declara que o objetivo último do Estado é tornar-se o "hegemon", reunindo para si todo poder que ele puder absorver para chegar até este estágio. (BALDWIN, 2013, p.283).

40 Vale ressaltar que, dentro das perspectivas realistas, a política internacional discute, principalmente, a política desenvolvida entre as Grandes Potências – a quem Simonds e Emeny (1937) identificaram como sendo os Estados com capacidades militares suficientes para acompanhar, com efetividade, a política externa designada por suas próprias decisões. Ela não preocupa-se em discutir política de Estados que não são considerados

2.2.2 Abordagem do Poder Relacional

O modo como a área das Relações Internacionais observava o poder até então – através da abordagem "dos elementos nacionais de poder" – alterou-se por volta da década de 1950 e passou a conceber o poder como fruto de uma relação.[41] Esta é a concepção central da abordagem do poder relacional. Em vez de o poder embasar-se na noção de **propriedade**, agora ele fundamenta-se na *causalidade*. (BALDWIN, 2013). Esta nova perspectiva do poder no sentido relacional também é adotada por Strange (1996), que admite a existência dos poderes relacional e estrutural – conforme será mostrado mais adiante.

A abordagem do poder relacional enxerga que o comportamento do ator A, ao menos parcialmente, provoca a alteração no comportamento do ator B. Por isto chama-se "relacional", visto que opera segundo causa e efeitos no contexto de uma relação entre dois atores. Aqui não cabe a noção de um poder derivado de recursos, capacidades, atributos do Estado. Além disso, o poder relacional compreende diferentes dimensões: Baldwin (2013) explica que, no mínimo, existem quatro – escopo, domínio, peso e custos.[42] De acordo com Jack Nagel (1975), quando se utiliza esta abordagem do poder relacional deve-se, no mínimo, explicitar as dimensões "domínio" e "escopo".

São dois grandes marcos dentro da abordagem do poder relacional: a corrente do Construtivismo e o debate das Faces de Poder. Enquanto o Construtivismo compreende três estudos relevantes (a inauguração teórica da corrente com Alexander Wendt, as noções de identidade e interesse desenvolvidas por Ted Hopf e a interpretação do poder "polimorfo" de Michael Barnett e Raymond Duvall), o Debate das

---

Grandes Potências. Isto porque as Grandes Potências podem dar-se "o luxo" de "pagar pra ver" o desenvolvimento da política externa pois suas próprias capacidades, traduzidas em poder militar, podem assegurar a operacionalização e manutenção dessa vontade política.

41 Baldwin (2013) explica que diversos estudiosos enxergaram a obra de Lasswell e Kaplan (1950), Power and Society, como marco revolucionário na área de RI – justamente por apresentar essa nova concepção do poder calcado na causalidade.

42 "Escopo" refere-se aos aspectos do comportamento de B que são afetados por A como, por exemplo, os aspectos econômicos. "Domínio" compreende o conjunto de atores que estão sujeitos à influência de A. "Peso" se refere a probabilidade de B ser afetado por A. E "custos" se referem aos meios pelos quais B é afetado por A (podem ser simbólicos, econômicos, militares, diplomáticos). (BALDWIN, 2013, p.275).

Faces de Poder compreende três momentos progressivos, pois a ideia é a de que o poder tem três faces. Para Baldwin (2013), este foi um dos maiores debates envolvendo poder no século XX. Ambos os marcos realizaram importantes considerações acerca do poder relacional.

Wendt (1992) aponta a existência de teorias sociais sobre interesses e identidades, negligenciadas pela disciplina de RI, e as agrega em um conjunto que chama de "construtivismo" – por vontade de enfatizar o foco na construção social da *subjetividade.* [43]

Ted Hopf (1998), observa que o Construtivismo agrega temas alternativos da agenda de RI: anarquia; balança de poder; relação entre identidade do Estado e interesse; elaboração do poder; prospecções de mudança na política global. Em especial sobre o poder, Hopf (1998) relembra que o Construtivismo argumenta que as noções de "poder material" e "poder discursivo" são necessárias para a compreensão dos assuntos internacionais. Ora, os Estados convivem em comunidade no SI e mantém relações de poder, direta ou indiretamente. Para o Construtivismo, não faz sentido debruçar-se, apenas, sobre o aspecto material, militar e bélico a fim de compreender a interação entre os Estados e a formação de balanças de poder. Faz-se necessário estudar o aspecto do poder que *deriva da relação entre eles*, sedimentada por práticas convencionadas dentro do SI (enquanto, por exemplo, Wendt buscaria compreender porque determinadas práticas tornaram-se convenção). Apesar de relevantes, os Estados, afinal, *não são os únicos atores deste sistema*. Este ponto curioso demonstra que algumas abordagens dentro da disciplina de RI têm a preocupação em trazer outros atores – que não o Estado – para o rol de estudos e pesquisas relevantes. Até então, os intelectuais preocupavam-se praticamente apenas com o Estado e os jogos de poder na arena política internacional.

43 Em 1992, Alexander Wendt publicou o artigo Anarchy is what states make of it. Neste artigo, ele observou que o debate entre os neorrealistas e neoliberais têm uma base comum – a "escolha racional". Esta escolha racional supõe que os estudiosos são "automaticamente" direcionados a fazer determinadas perguntas em detrimento de outras porque não existe questionamento sobre identidades e interesses. Não se pondera sobre estes pontos quando discute-se sobre atores na área de RI. Isso significa que os processos e as instituições podem até mudar o seu comportamento próprio, mas os estudos sobre eles preservam suas identidades e interesses – são estáticos, não há questionamento. (WENDT, 1992).Wendt (1992) sugere dois caminhos de estudo: primeiro, que a resposta para essas inquietações dependem, em parte, no quão importante são as interações entre os Estados para a constituição de suas identidades e interesses. Segundo, também depende do quão fácil acontecem as mudanças de interesse e identidade dos Estados frente às interações sistêmicas. (Ibid., p.423)

Já os norte-americanos Michael Barnett e Raymond Duvall (2005) interpretam o poder como "polimorfo", ou melhor, ELE apresenta-se em diferentes formas.[44] Eles oferecem uma explicação para o poder ser tratado, em RI, basicamente pelo guarda-chuva teórico do Realismo (algo que Strange também faz).[45] Para estes autores (Ibid., p.45-46) o poder pode ser expressado de duas formas: através da interação (ou seja, a partir de causa e efeito); ou através da constituição dos atores como seres sociais (neste caso, o poder opera através de relações *sociais*) Eles concluem que essa distinção conceitual é muito similar à distinção sobre poder na literatura da área que argumentam sobre "power over" e "power to".

Finalmente, o Debate das Faces de Poder compreende considerações acerca da primeira face, segunda face e terceira face do poder. O debate acerca da "primeira face do poder" se inicia com os estudos de Robert A. Dahl (1961) na obra *Who Governs? Democracy and power in an american city*. Neste estudo, Dahl (1961) busca compreender quem governa na cidade de New Haven, no estado de Connecticut, nos Estados Unidos. Em suma, a "primeira face do poder" tem um foco: determinar quem tem o poder de lançar propostas políticas na tomada de decisão de um assunto determinado. A segunda face do poder relaciona-se com os estudos de Bachrach e Baratz (1962): ambos argumentam que existe conjuntos de assuntos que nunca serão levados à mesa de decisão porque, na primeira face, os assuntos já foram tomados como dados. Mas existem outros que não são selecionados. Esta negligencia reflete o debate da segunda face do poder: a habilidade que o poder tem de selecionar quais assuntos serão discutidos no processo de tomada de decisão. Finalmente, a terceira face do poder foi apresentada por Lukes (1974) como sendo o modo por meio do qual o ator A causa mudança no comportamento de B. Existem diferentes formas – A pode

44 Os quatro tipos de poder formulados por eles (Ibid., p.43) são: poder compulsório; poder institucional; poder estrutural; e poder produtivo. O poder compulsório é o poder como relações de interações de controle direto de um ator sobre o outro. O poder institucional é o controle direto que os atores exercem indiretamente sobre os outros através de difusas relações de interação. O poder estrutural é a constituição das capacidades do sujeito em relação direta estrutural de um com o outro. E, finalmente, o poder produtivo é a produção socialmente difusa da subjetividade nos sistemas de significado e significação.

45 Os autores sugerem que os realistas, essencialmente, tratam o poder como um recurso material de coerção cujo intuito seja influenciar o ator B a alterar seu comportamento. De acordo com eles, a tendência em associar poder com a corrente teórica realista, na área de RI, se deve ao fato de que praticamente são eles os únicos que versam sobre o poder de fato. Sem a existência de considerações sobre poder em outras esferas, o Realismo triunfa quase que hegemonicamente quando se trata das Teorias das Relações Internacionais. (BARNETT; DUVALL, 2005).

afetar necessidades, pensamentos, desejos e até as preferências de B. Lukes (1974) admite a semelhança da terceira face do poder com os estudos de Antonio Gramsci, acerca da "hegemonia", e Joseph Nye, "poder brando".

2.3 RUPTURA COM A TRADIÇÃO TEÓRICA DE RI

Tanto pela abordagem dos elementos nacionais de poder, quanto pela abordagem do poder relacional, a unidade de análise tratada pelas correntes teóricas tradicionais em RI fora quase exclusivamente o Estado-nação. Para Strange (1996) isto era incômodo na medida em que distanciava a teoria da prática real do cotidiano: atores não-estatais proliferavam no SI com bastante autoridade sobre diferentes temas.

Quando Morgenthau (1948) discorreu sobre a balança de poder, e trouxe uma visão de que o poder poderia ser "mensurado", tratava do poder do Estado no cenário internacional: o poder é cabível de mensuração a partir dos recursos de um Estado. Waltz (1979), por sua vez, compreende o cenário internacional a partir de uma estrutura política definida – com princípio ordenador, diferenciação das unidades e especificidade de suas funções, e distribuição de capacidades entre as unidades. Neste SI, os *Estados* podem ser classificados de acordo com o poder que "possuem", pois os recursos de poder são as próprias capacidades do Estado. Já Mearsheimer (2001) retoma a ideia da balança de poder, evidenciando a posição privilegiada do Estado neste contexto do SI. Os Estados são os agentes que buscam defender a sua balança de poder ou enfraquecê-la (se isto os favorece de alguma forma).

Em nenhuma das correntes teóricas dentro da abordagem dos elementos nacionais de poder admite-se a relevância de outros atores que não fossem o Estado. Afinal, sendo os elementos "nacionais", não admite-se (e nem preocupa-se) com a existência de elementos que não fossem atribuídos ao Estado. Assim, enquanto soberano, o Estado, além de único "player", também via na anarquia a razão de assegurar-se como entidade independente capaz de sobreviver no SI. Estas correntes não explicavam, nem pretendiam explicar, o desenvolvimento, o poder ou a sobrevivência de corporações transnacionais ou qualquer outro ator não-estatal com autoridade no cenário internacional. E, ainda assim, estas correntes mantiveram-se como pilares fundamentais sobre os quais se

edificou a disciplina de RI – que, cabe lembrar, discutiu a política internacional sem, até então, considerar atores políticos não-estatais.

Logo na sequência surgiu a abordagem do poder relacional. Ela flexibilizou a observação do poder porque admitiu, pela primeira vez na área de RI, que o mesmo não era derivado apenas de elementos nacionais. O poder relativo surgiu a partir da concepção de uma ideia de causalidade: é o exercício de influência que A tem sobre B de modo a alterar o comportamento de B para aderir a resultados desejados por A. Esta concepção de poder rompe com a noção anterior assentada sobre elementos nacionais. Enquanto antes se via o poder como recurso, elemento de posse, a nova abordagem pretendeu conceder um sentindo causal de poder, derivado de uma relação. Mas, semelhante à abordagem dos elementos nacionais, as análises que utilizavam a abordagem do poder relacional comumente tratava a política internacional como arena dos Estados. Grosso modo, faltava às duas abordagens o reconhecimento e a explicação da existência de poder e autoridades oriundas do Mercado – ou melhor, do setor privado. É aqui que as contribuições de Strange se tornam evidentes. Ela reconhecia que, na prática, inúmeras autoridades não-estatais detinham poder sobre atividades e pessoas no SI. Sobre isso, ela afirmou que "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).

Como poderia Strange explicar a existência, e o poder, de autoridades não-estatais no SI a partir de uma literatura tradicional de RI? Como poderia discutir política internacional sem considerar a dimensão dos atores não-estatais, reconhecendo-os como autoridades com poder sobre atividades e pessoas no cenário internacional? Ao que tudo indica, não pôde. E por esta razão, ela rompeu com a disciplina de RI para dedicar-se ao estudo da política internacional a partir do campo de estudo da EPI. Embora, houvesse algumas abordagens que buscavam tratar de atores não-estatais, o fato era que dentro da disciplina de RI, o Estado permanecia como centro das análises sobre política internacional. E sobre isto, ela afirmou

> 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 nternational 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)

Para Strange (1988), as análises da política internacional necessitavam abranger as práticas vividas no cenário internacional – e isso incluía a existência de atores não-estatais e o poder que estas autoridades exerciam sobre pessoas e atividades. Por esta razão, buscava assentar suas análises a partir de três premissas fundamentais:

> […] Politics is a common activity; it is not confined to politicians and their officials. The second is that power over ally 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).

A primeira premissa abre espaço para considerações políticas além do palco regido pelos governos nacionais e organizações internacionais – o que inclui a política feita por empresas multinacionais, corporações e organizações transnacionais e demais autoridades. A segunda premissa indica que o poder não advém, apenas, das relações políticas mas também das relações econômicas e financeiras. O capital abre oportunidade para o exercício do poder. A terceira premissa retira a exclusividade da autoridade dos Estados sobre as pessoas e atividades dentro de suas fronteiras geográficas. Esta última premissa visa derrubar, tanto quanto possível, as largas diferenças entre a prática do cotidiano e as teorias e análises realizadas nos centros acadêmicos ao redor do mundo. Com estas três premissas em vista, o leitor poderia compreender tanto a ecleticidade de Susan Strange quanto ponderar sobre a relevância da "simbiose" das disciplinas da Política e Economia para as análises das Relações Internacionais – afinal, poder e capital caminham juntos no cenário global.

A seguir serão apurados os estudos acerca do "poder" e "difusão de poder" que surgiram na EPI a partir da inglesa Susan Strange, ao final da década de 1980 e meados da década de 1990. As revisões sobre o elemento "poder" tratadas até aqui ajudam a compreender as razões pelas quais Strange (1988) formula a noção do poder estrutural e como se encaixa na leitura sobre poder dentro das Relações Internacionais. O triunfo de Strange (1988) talvez tenha sido contribuir para a noção de que o poder reside, também, em atores não-estatais no contexto do SI. Para isso, Strange (1996) não recorreu à criação de uma teoria alternativa sobre poder que pudesse explicar novos atores. Segundo Palan (1999), ela utilizou do seu próprio ecleticismo para criar um "framework" a partir do qual as análises sobre a realidade prática do SI (e dos fundamentos que assentam a condição humana) pudessem ser examinadas. Este "framework" foi pensado por ela a partir de valores básicos humanos enquanto organização social: riqueza, segurança, liberdade e justiça. (STRANGE, 1988). Dessa forma, a abordagem de Strange sobre o elemento do poder é a partir de uma visão holística – razão pela qual Palan (1999) acredita que o conceito de poder estrutural não possa ser utilizado de modo independente do "framework" das quatro estruturas elaboradas por ela. Afinal, o poder estrutural não emana das quatro estruturas (segurança, produção, finanças e conhecimento), mas é a própria articulação de elementos oriundos delas. (PALAN, 1999).

A seguir, temos três objetivos: (1) definir as quatro estruturas primárias descritas por Strange (1988), com especial atenção à estrutura do conhecimento; (2) apresentar o conceito de poder estrutural; (3) descrever o fenômeno da difusão de poder. Estes assuntos encontram-se em duas obras principais da autora: *States and Markets*, 1988, e *The Retreat of the State: The Diffusion of Power in the World Economy*, 1996. Esta última obra é considerada por ela como "an extension, or elaboration, of the same ideas about power and transnational relations that characterise the contemporary world scene." (STRANGE, 1996, p.x). As ideias sobre poder e relações transnacionais são vistas na primeira obra, *States and Markets*.

2.4 O PODER ESTRUTURAL

Em 1988, Susan Strange apresentou o conceito de poder estrutural na obra *States and Markets*. Este conceito surge como uma interpretação alternativa de poder aos conceitos existentes na literatura de RI. Para ela, dois poderes são exercidos dentro de uma Economia Política: poder relacional e poder estrutural. No entanto, mesmo reconhecendo a existência e o exercício do poder relacional, ela aponta que o poder estrutural tem tido maior relevância no SI.

Strange define o poder estrutural e realiza algumas considerações acerca do mesmo. Ela afirmou que

> 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).

O poder estrutural origina-se a partir das quatro estruturas mencionadas na seção anterior. As estruturas não emanam poder, mas é

a partir da articulação de elementos provenientes destas estruturas que o poder estrutural é concebido. Por esta razão, tanto Palan (1999) como Brown (1999) não consideram Strange uma teórica: ela não cria uma teoria alternativa, ela fornece insumos suficientemente capazes de ofertar uma visão de mundo sobre os atores (estatais ou não) e suas atividades a partir de estruturas inter-relacionadas (e estas concebidas a partir de valores básicos da organização humana). É a partir desta visão estrutural do SI que os atores relacionam-se. Esta visão estrutural permite, sobretudo, trazer atores não-estatais para os estudos acadêmicos em EPI – algo inconsistente com a disciplina de RI até aquele momento. A relevância destes atores na obra de Strange é demasiada porque (1) reflete a prática política e econômica encontrada no cotidiano dos cenários internacionais, onde empresas multinacionais (e outras organizações ou mesmo indivíduos) mantêm acordos e exercem influências sobre governos, pessoas e organizações; (2) demonstra que, dentro de cada estrutura (segurança, produção, finanças e conhecimento), o Estado não é o *único* ator e muito menos o mais relevante a ponto de assumir o topo, a liderança, da estrutura. Pelo contrário. Em obra posterior, Strange (1996) admite que o Estado assume a posição de liderança em apenas **uma** estrutura: a da segurança. (STRANGE, 1996). Nas demais estruturas, o Estado atual é apenas um dos atores relevantes que exercem influência e buscam poder – não é único.

As quatro estruturas não se fazem presentes apenas no contexto internacional. A concepção do poder estrutural é assentada por meio de um quadro de análise, ou melhor, um método por meio do qual se realizam diagnósticos sobre a condição humana afetada por circunstâncias sociais, políticas e econômicas. (STRANGE, 1988). Haja vista que tais circunstâncias descrevem, inclusive, o contexto local, o poder estrutural está disseminado pelo tecido econômico-político em diversos níveis. Inclusive, por esta razão, pode-se analisar, através da concepção de poder estrutural, as relações humanas que ocorrem em famílias, bairros ou tribos humanas – desde que estas relações decorram de circunstâncias sociais, políticas ou econômicas.

Ademais, observamos, a partir da citação acima, que o poder estrutural **recai** sobre aqueles que estão em posição de **controle** no contexto de, pelo menos, uma estrutura primária (segurança, produção, finanças e conhecimento). Sobre isso, Strange (1988) afirmou que

> 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).

Ou seja, se trata sobre ter o controle de um objeto diante de, pelo menos, uma estrutura primária – no contexto local e/ou global. Tanto na rua do bairro, quanto sobre um bairro, ou ainda nacionalmente ou globalmente. E mais: Strange (1988) indica que o possessor do controle da estrutura (em seu nível macro ou micro) pode exercer o poder **sem**, de modo aparente, colocar pressão diretamente nos demais para tomarem uma decisão ou fazer uma escolha entre as alternativas. E isto é possível porque o poder estrutural apesar de ser menos "visível" (que o poder material, por exemplo) ainda é presente.

Contudo, muitos poderão questionar: se o poder estrutural deriva de articulações oriundas a partir de quatro estruturas inter-relacionadas – e não exclusivamente de modo individual – como ele pode recair sobre um ator que exerce controle sobre o aspecto de pelo menos uma estrutura? Strange não fornece uma resposta, mas podemos arriscar um palpite. O poder estrutural foi representado, metaforicamente, por Strange como uma pirâmide tetraédrica cujas faces representam as estruturas primárias (segurança, produção, finanças e conhecimento). E, apesar de originar-se a partir da dinâmica dos elementos oriundos das estruturas, pode ser "observado" a partir de uma das faces do tetraedro, ou melhor, a partir de uma estrutura. Em outras palavras, embora seja compreendido pelas quatro estruturas (que complementam e relacionam-se entre si), existe a possibilidade de observar o poder estrutural originando-se, especificamente, no contexto de uma das estruturas. Ele não se origina isoladamente a partir de uma única estrutura, mas o foco de análise do poder estrutural pode estender-se para uma das estruturas.

É possível mover a pirâmide de modo a examinar em detalhes cada uma de suas faces.[46]

2.5 AS QUATRO ESTRUTURAS PRIMÁRIAS

Susan Strange (1988) definiu quatro estruturas primárias: estrutura da segurança; estrutura das finanças; estrutura da produção e estrutura do conhecimento.[47]

A **estrutura da segurança** é o "quadro de poder" criado a partir da provisão de segurança de alguns seres humanos para outros seres humanos. (Ibid., p.45). Segue um exemplo que tomamos a liberdade de formular a partir do convite ao estímulo criativo realizado pela própria autora no contexto de suas obras.

Imagine uma época pré-histórica em que os seres humanos divagavam em bandos sobre a terra e precisavam se proteger de ameaças do clima, dos animais, doenças, acidentes geográficos, outros grupos humanos, etc. Aquele indivíduo, dentro do grupo, que fosse capaz de fornecer segurança para o(s) outro(s) que, por exemplo, estão sendo ameaçados por um inimigo, ganha "poder estrutural" dentro deste "quadro de poder". Ele é capaz de afetar os resultados (protegendo o seu bando do inimigo, o resultado é que o seu grupo está salvo – diferente de outro possível resultado, que é a morte do bando) de modo que sua preferência (salvação do bando) tenha precedência sobre a preferência do outro (morte do bando). O controle sobre a segurança do grupo confere a este indivíduo "salvador", poder estrutural, que origina-se por meio da estrutura de segurança. O seu bando, e o bando inimigo, passarão a enxergá-lo como um agente "poderoso" e pensarão duas vezes: antes de fazer incursões violentas sobre ele (segurança); ao produzir algum bem que seja de seu interesse (produção), já que existe o

46 Ver "Anexo 1 – Pirâmide Representativa do Poder Estrutural".

47 Existem também as estruturas secundárias: sistemas de transporte transnacionais, sistema de comércio, sistemas de fornecimento de energia e sistema de bem-estar social e desenvolvimento transnacional. (Ibid., p.139). A britânica admite que a escolha dessas estruturas são um pouco "arbitrárias no sentido de que seria igualmente lógico incluir algumas outras estruturas secundárias". (Ibid., p.139, tradução nossa). A característica principal dessas estruturas secundárias é que, apesar de serem quadros de ações dentro dos quais as escolhas são feitas baseadas em preferências por valores, também são secundárias às quatro estruturas primárias de segurança, produção, finanças e conhecimento. Quando se trata do poder estrutural, ela formula a analogia da pirâmide.

risco a integridade física daquele que produzir o bem (afinal, para conquistar o bem, ele pode ameaça-lo); e àquele que fornecer "empréstimos" ou créditos na forma de alimento, vestimenta, etc., devido aos riscos a integridade física. A relação entre este ator e o seu próprio bando, e ele em relação aos bandos inimigos, se altera – mesmo que o indivíduo "salvador" não tenha consciência disso.[48] E esta relação se altera porque, uma vez que ele é visto como um agente "poderoso", a sua mera presença será capaz de operacionalizar este poder.

No nível micro, isto pode acontecer tanto no contexto da pré-história, em grupos humanos pequenos, quanto no contexto de periferia de uma cidade da era atual. No nível macro, isto acontece tanto do ponto de vista doméstico, quando o Estado reúne para si o uso legítimo da força na sociedade, quanto do ponto de vista internacional, quando procura alterar o equilíbrio de poder estrutural entre os atores. De acordo com Strange (1988), no contexto do sistema internacional atual, a estrutura de segurança é concebida ao redor da instituição do Estado, mesmo que ele não haja de modo isolado no sistema. (STRANGE, 1988).

A **estrutura da produção** pode ser definida "as the sum of all the arrangements determining what is produced, by whom and on what terms." (STRANGE, 1988, p.64). Ou seja, na perspectiva da EPI de Strange, a estrutura da produção é responsável por criar a "riqueza". Quando esta estrutura se altera, "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). É natural que estas mudanças ocorram uma vez que a estrutura da produção está no cerne da organização da vida em sociedade. Cada vez mais, a estrutura de produção no contexto global é caracterizada por empresas transnacionais. Quanto a isso, Strange (1988) afirmou que "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).

A **estrutura das finanças** é definida de acordo com os atores capazes de criar ou negar concessão de crédito aos demais e sem os quais não é possível o funcionamento de nenhuma economia avançada. (STRANGE, 1988). Se observamos esta questão a partir do nível micro, percebemos que "the power to create credit implies the power to allow or to deny other people the possibility of spending today and paying

48 Nota-se aqui a contribuição dos estudos de gênero para a EPI, conforme mencionado por Strange (1988).

back tomorrow" e no nível macro "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). De modo reflexivo, aquele que tem controle sobre o crédito é capaz de afetar direta, ou indiretamente, o escopo das escolhas dos demais.

A **estrutura do conhecimento** é definida por Strange (1988) da seguinte forma:

> [...] 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).

Esta estrutura está relacionada com o conhecimento produzido, descoberto, armazenado e comunicado. Veja que Strange (1988) não faz diferenciações conceituais entre "conhecimento" e "informação", desde que esta unidade seja considerada socialmente relevante. Àqueles que detêm o conhecimento relevante e desejado, e também àqueles que de alguma forma controlam os canais de comunicação e armazenamento destas informações, é conferido de poder estrutural que origina-se a partir da estrutura do conhecimento. Além do poder, também são conferidos a eles autoridade.[49] Estes dois elementos, poder e autoridade, são conferidos à estes indivíduos em razão de ocuparem posições importantes dentro da estrutura porque além de serem tomadores de decisão, também são reconhecidos como detentores do conhecimento desejado pela sociedade (e que, portanto, tem valor para o organismo social). Podemos assumir alguns exemplos oriundos da estrutura do conhecimento como pesquisadores, criadores de conteúdo, profissionais de biblioteconomia, sistemas de informação, cientistas da computação, etc., enfim, a classe de profissionais (e expoentes de destaque em uma determinada área do conhecimento) que estão relacionados, direta ou indiretamente, com a produção, comunicação e armazenamento do conhecimento (ou informação) considerada socialmente relevante. Estas

49 Esta distinção semântica entre "poder" e "autoridade" nesta citação de Strange é relevante para a compreensão da autoridade como uma dimensão em si mesma. Isto será discutido em momento posterior.

figuras são consideradas "autoridades" dentro da estrutura do conhecimento. E para ser uma autoridade é necessário, primeiro, que o ator tenha, de fato, o dito conhecimento relevante; e que, segundo, tal conhecimento seja considerado importante. (STRANGE, 1988).

Alguns exemplos apresentados por Strange (1988) evidenciam atores passados que obtiveram êxito no acúmulo de poder estrutural, oriundo principalmente da estrutura do conhecimento, ao longo dos anos: a Igreja Católica durante o período medieval e o Estado cientificista do século XX. A Igreja Católica detinha autoridade e poder porque, entre outros pontos importantes, controlava os meios de comunicação (que abrangiam toda a Europa medieval), pelos quais se transmitia o conhecimento, na forma de livros sagrados e alfabetização na língua sagrada Latim. Aqueles a quem era permitido o acesso ao armazenamento de conhecimento – os livros sagrados guardados pela Igreja – necessitava, além do acesso, conhecimento do idioma em que a informação estava inscrita. Veja que é a Igreja Católica que controlava, durante a época medieval, os meios de comunicação e armazenamento – além de investigar descobertas e negar o acesso ao conhecimento a outros indivíduos. O Estado cientificista, por outro lado, era apontado por Strange (1996) como a instituição que assumiu algumas responsabilidades da Igreja Católica referentes a estrutura do conhecimento (como o crescimento do sistema educacional que permitiu acesso à educação em escolas e universidades) e investiu em inovações técnicas (da qual descobriu-se novos conhecimentos em diversas áreas, especialmente a Física) e por meio dos quais deu origem ao direito de propriedade intelectual. (STRANGE, 1988).

A estrutura do conhecimento também é um pouco diferente das demais estruturas por algumas razões: (1) Strange (1988) afirma que o poder que se origina a partir da estrutura do conhecimento é compreensivelmente difuso; (2) é um poder dito por ela "inquantificável";[50] (3) o poder derivado da estrutura do conhecimento

[50] A interpretação que faço disso é a de que nas outras estruturas, o poder que origina-se a partir delas ainda é passível de quantificação – mesmo que grosseiramente. Na estrutura das finanças, por exemplo, é possível ter uma noção da "quantidade" de poder através de uma análise bancária sobre a concessão de crédito. Em uma perspectiva micro é possível ter uma noção do poder estrutural por meio do exame de quanto foi "emprestado" para um indivíduo. Essa quantia financeira determina o poder de compra do indivíduo que recebeu o crédito e oferece uma ideia da intensidade de poder do credor. Na estrutura de produção, em contrapartida, podemos ter uma razoável ideia da "quantidade" de poder por meio do quanto foi produzido (ou deixado de produzir), do quanto foi fabricado, confeccionado. Na estrutura da segurança, essa percepção de "mensurável" de poder acontece por meio da análise, por exemplo, do tamanho dos exércitos, da quantidade de recursos bélicos de

assenta-se, também, na negação de acesso ao conhecimento; (4) é um poder mais associado ao consentimento do que a coerção – diferente das outras estruturas; (5) é necessário existir reconhecimento social de que aquela informação seja considerada importante – de modo que a pessoa detentora deste conhecimento também é considerada relevante à sociedade. (STRANGE, 1988).

Finalmente, devemos compreender que as estruturas não são estáticas, elas são dinâmicas e estão sujeitas a mudanças e desenvolvimentos. Quanto a isso, Strange (1988) admite que, de todas as estruturas, a estrutura do conhecimento é aquela que está passando por mudanças mais rápidas ao final do século XX.[51] E embora não tenha versado, especificamente, sobre a Internet quando realizou considerações acerca da estrutura do conhecimento, Strange reconheceu a relevância da revolução da informação que ocorria ao final do século XX.[52] Em especial, salientou a importância da combinação de três áreas tecnológicas que passavam por grandes mudanças: os sistemas de computadores disponíveis e com baixo custo; os sistemas de comunicação via satélites em órbita em larga escala; e a digitalização da linguagem, que abre potencial para a derrubada de barreiras idiomáticas entre grupos humanos. (STRANGE, 1988). E, ao final, concluiu que a interação entre as estruturas sugere conclusões políticas muito

---

um Estado, do número de armamentos nucleares. A posse de 50 ogivas nucleares e "nenhuma" ogiva nuclear é um indicativo, grosso modo, do poder que determinados Estados na oferta de segurança ou ameaça de violência. No nível micro, observamos o número de membros que compõem uma gangue de rua e a quantidade de recursos que possuem tanto para proteger, quanto para ameaçar terceiros. Mas, na estrutura de conhecimento, é compreensivelmente difícil quantificar o "quanto" de conhecimento um indivíduo, ou grupo de indivíduos, possui. O conhecimento e a informação não se traduzem em números de livros, artigos, revistas, jornais, etc., afinal, estes números não significam, automaticamente, em conhecimento absorvido e comunicado. Esta é a dificuldade de mensuração do poder estrutural que se origina a partir da estrutura do conhecimento. Devemos apontar, no entanto, que Strange (1988) indica que o controle de canais de comunicação (e também armazenamento) por onde informações, conhecimento e crenças são comunicados também conferem poder estrutural. Desse modo, aquele que permite, ou nega, o acesso dos demais a estes canais de comunicação tem poder. Este ponto talvez seja o único que permita a ilustração da "quantidade" de poder que se origina a partir da estrutura do conhecimento: uma empresa privada global que permite, pelo uso da tecnologia, milhões de pessoas comunicarem-se utilizando seus canais de comunicação (e-mails, servidores, plataforma de chats, "office" compartilhado, etc.) e decide alterar a política de acesso é detentora de poder estrutural pois afeta diretamente as opções de ação dos clientes. Mesmo assim, é apenas um indicativo do poder.

51 Strange escreve sobre as estruturas primárias no contexto da obra de 1988, ou seja, também ao final do século XX.

52 Susan Strange faleceu em 1998, de modo que não versou especificamente sobre os sistemas de informação digitais que culminaram na ascensão da Internet comercial.

importantes: as inovações tecnólogicas em curso resultavam na unificação global de bens e serviços. (Ibid., p.130). Embora o mundo já tenha vivenciado a unificação de mercados, estes eram limitados pelos sistemas de transporte. A nova dinâmica, calcada na microeletrônica, é diferente: os novos meios de comunicação permitem que a informação seja acessível a compradores e vendedores globalmente – e também permite que as decisões de compra e venda, bem como a execução destas decisões, sejam realizadas de modo instantâneo. Portanto, isto implica em consequências políticas e econômicas inovadoras. (Ibid., p.131).[53]

Strange (1988) demonstra estar ciente de suas limitações em relação à estrutura do conhecimento. Em parte porque reconhece que o poder derivado da estrutura do conhecimento é o mais negligenciado dentre todos (segurança, produção e finanças) nos estudos de psicólogos sociais, filósofos, especialistas em tecnologias, etc. Sendo assim, há pouco insumo para análises que partem da estrutura do conhecimento. E em parte porque a mudança que ocorre na estrutura do conhecimento é a mais veloz dentre todas as estruturas e, por esta razão, os resultados ainda não são claros. Mas, apesar disso, assegura que existem evidências suficientes para sustentar que a estrutura do conhecimento está passando por, pelo menos, três amplas alterações.

O primeiro deles é tem a ver com a própria relevância da estrutura do conhecimento. Strange (1988) afirma que ao final do século XX, a estrutura do conhecimento é considerada tão importante que a competição entre os Estados no SI pode ser entendida como uma competição pela liderança desta estrutura. No passado, isto não era verdade: os Estados competiam por território. E a competição por território acontecia porque a produção de riqueza (e, portanto, aquisição de poder) dependia de terra e de recursos naturais. O século XX alterou esta concepção competitiva: os Estados buscam a liderança do desenvolvimento tecnológico de ponta. (Ibid., p.136). Segundo ela,

53 Algumas dessas implicações econômicas e políticas são: a relevância da informação para a estrutura da produção é aumentada significativamente e, com isso, a revolução da informação desvaloriza o poder e a riqueza dos trabalhadores industriais (ou seja, menos pessoas trabalhariam no chão da fábrica, minas, fazendas, navios e etc., e mais pessoas inseridas em escritórios com computadores e processadores – menos "colarinhos azuis" e mais "colarinhos brancos"); as grandes empresas de manufatura seriam obrigadas a diversificar em setores informacionais; nas empresas, o valor do trabalhador "de conhecimento" é aumentado às custas do valor de trabalhadores industriais; o poder e as capacidades da gerência em grandes empresas é realçada; as empresas seriam capazes de aumentar significativamente a internacionalização da informação; etc. (STRANGE, 1988, p.131-133).

existe o reconhecimento popular de que "conhecimento é poder" há bastante tempo mas falta aos teóricos de RI e EPI absorverem esta realidade dentro da academia.

O segundo desenvolvimento refere-se no aumento da assimetria entre os Estados como autoridades políticas na aquisição de conhecimento e de acesso a ele. (Ibid., p.137). No SI, os Estados apresentam-se como autoridades políticas soberanas e iguais – mas o acesso e a aquisição de conhecimento não se dão de forma igual.

O terceiro desenvolvimento, pouco explorado pela autora, diz respeito a novas distribuições de poder, status social e influência para além das fronteiras estatais – em razão da estrutura do conhecimento. (STRANGE, 1988). Segundo ela, por exemplo, é a quantidade de nacionais com acesso à educação superior que diferencia os Estados. O acúmulo de educação, informação, conhecimento retira os obstáculos do acesso ao crédito (e não apenas o acúmulo de riqueza em qualquer forma). E afirma ainda que está ocorrendo uma alteração na transmissão do poder: gradualmente, o poder está deslocando-se das nações "ricas em capital" para aquelas "ricas em informação". Por esta razão, ela considera que o aceso ao conhecimento está no cerne do status social e distribuição de poder. (Ibid., p.138).

2.6 DIFUSÃO DE PODER

Tendo versado sobre o poder relacional, o poder estrutural e as estruturas primárias definidas por Strange (1988), cabe-nos agora expor o fenômeno da difusão de poder. Este fenômeno é tema da obra *The Retreat of the State: The Diffusion of Power in the World Economy*, de 1996. Apesar da expressão "difusão de poder" aparecer no título, ela aparece apenas uma vez em todo o conteúdo da obra. [54] Entretanto, é

54 Ela utiliza a expressão "difusão de poder" quando trata de empresas de telecomunicação. Destacamos o trecho a seguir: "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).

bastante comum o termo “difusão” aparecer associado à palavra “autoridade”.

Segundo Strange (1996) é difícil definir autoridade. Explicitamente, ela não define este conceito em nenhuma das duas obras. Entretanto, há duas passagens distintas que nos elucidam quanto ao significado. Primeiro, (1) em *States and Markets*, quando discute o uso mais abrangente do termo “política”: “[…] 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, grifo nosso). E, segundo, (2) em *The Retreat of the State*, quando investiga como identificar quem é autoridade no cenário político-econômico global: “[…] 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, grifo nosso).

Na primeira passagem, as autoridades são aquelas entidades com poder suficiente para alocar valores no contexto social, político e econômico. Estes valores, segundo Strange (1988), são aqueles oriundos da organização social humana: segurança, riqueza, justiça e liberdade de escolha – considerados por ela como os quatro valores básicos da economia política. (Ibid., p.5).

Na segunda passagem, podemos identificar qual o significado de autoridade para Strange (1996). Ela deixa claro que as autoridades à que se refere são entidades que têm poder suficiente para alterar os resultados e definir as opções para os demais – o que está de acordo com a primeira passagem, mas adiciona o aspecto relacional de influência sobre os resultados. Por definição, portanto, no quadro analítico desenvolvido pela EPI, presume-se a existência de outras autoridades além do Estado: ele não é o único com poder de alocar valores, redefinir as opções para os demais e nem de influenciar os resultados. O grande teste, no entanto, aquilo que determina se uma entidade tem autoridade (de fato, e não potencial) são os resultados. (STRANGE, 1996, p.91). Em outras palavras, perceber um ator não-estatal como autoridade, dentro de um contexto, é um exercício de análise sobre a influência dele sobre os resultados.

De acordo com Strange (1996), no cenário econômicio-político do século XX, o poder de alocar valores e alterar os resultados para os demais estava, essencialmente, concentrado na figura do Estado-nação.

O início da concentração de autoridade no Estado-nação começou a partir do Tratado de Vestfália. Antes disso, grande parte da autoridade estava concentrada na Igreja Católica.[55]

A difusão de poder é o fenômeno inverso: o poder do Estado-nação – tanto em alocar valores quando exercer poder sobre resultados, a partir de um quadro analítico da EPI – difunde-se pelo tecido social, político e econômico para outras autoridades que, ora rivalizam com o Estado, ora o reforçam.[56] Em outras palavras, "[…] 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). E, especialmente, ao final do século XX o fenômeno da difusão de poder surge com destaque: "[...] Authority over society and economy is 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). Portanto, se observamos cada uma das estruturas primárias que compõem o quadro de análise da EPI, percebemos que a autoridade encontra-se compartilhada com outros atores. Em suma, também podemos identificar o fenômeno da difusão de poder, de modo sintetizado, na hipótese da obra de 1996, em que afirma

55 De acordo com ela, "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 A classificação destas autoridades apenas ocorre em relação ao próprio ator estatal. Strange (1996) sugere classificar as autoridades existentes em relação à autoridade do próprio Estado. Desse modo, imaginemos uma reta contínua em que esteja alocado, em um extremo, a autoridade não-estatal que contesta e desafia (ou mesmo ameaça substituir) a autoridade do Estado. E no outro extremo desta mesma reta a autoridade não-estatal que sustenta e reforça a autoridade do Estado. No meio desta reta, alocam-se autoridades que exercem ou reforço, ou rivalidade, em relação à autoridade estatal. Se as autoridades estão mais para cá, ou para lá, da reta, é o Estado quem diz pois a percepção de rivalidade ou reforço é feita pelo próprio Estado. Essa percepção é bastante subjetiva e passível de alteração. (STRANGE, 1996, p.92) A partir disto, sugerimos alguns exemplos: os seguranças de casa noturna, vigilantes profissionais de rua, empresas de segurança, são exemplos de autoridades (formais porém não-máximas) dentro da estrutura da segurança que sustentam e reforçam a autoridade do Estado ao prestar serviços de proteção a outros atores (que podem ser pessoas, grupo de pessoas, empresas, propriedades, etc.). Penso que exemplo de rivalidade, neste caso, é o chamado "estado paralelo", ou seja, grupos criminosos organizados que ofertam proteção e ameaça de violência a pessoas, grupos de pessoas, empresas, propriedades, etc.

> 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)

O fenômeno da difusão de poder apresentada por Strange (1996), segundo ela, explica movimentos econômico-políticos que ocorreram na segunda metade do século XX, como o cenário mundial após os choques do petróleo e a inflação. As correntes tradicionais de RI não buscaram explicar este momento. Em especial, o foco de sua narrativa trata sobre a economia dos EUA. Segundo a britânica, neste período tanto a economia estadunidense cresceu e se "espalhou" pelo mundo, quanto as fontes do seu poder – que se deslocaram da "terra" e das "pessoas" para se assentar no controle sobre as estruturas do sistema global.

De modo detalhado, Strange (1996) discute a desordem provocada pelas inflações que se seguiram após os choques de petróleo a partir de uma visão global das estruturas – que neste caso é o SI no qual operam atores estatais e não-estatais. Existe o reconhecimento da relevância dos atores não-estatais, uma vez que estão imbuídos de poder estrutural. Contudo, a disciplina de RI, e em especial as correntes teóricas tradicionais da área, não conseguem explicar este mesmo cenário porque comumente atribuem ao Estado a unidade de análise política. É esta perspectiva política – de que o Estado é o ator supremo na política internacional – que colide com a perspectiva econômica, pois este último admite a relevância de atores não-estatais, passíveis de análise. Por esta razão, qualquer análise de EPI deve expandir a unidade de análise política pois, se o lócus de poder migra da "terra" e das "pessoas" para o "controle" sobre elementos oriundos das estruturas do sistema global, o ator que esteja de posse deste controle é dito

"autoridade" nesta estrutura.[57] Sobre a importância de admitir análises sobre atores não-estatais, Strange (1996) argumenta que

> Extending the focus of analysis from states to all for is 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).

Ao estender o foco de análise do Estado para outras formas de autoridade, a EPI se separa da disciplina de RI, no sentido tradicional. A adoção de uma definição de política mais abrangente, que leva em consideração todas as formas de autoridade (incluindo todos aqueles capazes de alocar valores), permite a união da Política e da Economia de modo a serem tratados como algo único ao invés de duas áreas separadas.

2.7 AS TRÊS DIMENSÕES DA DIFUSÃO DE PODER

Quando Strange (1988, 1996) discorreu sobre poder estrutural, estruturas primárias, autoridades e difusão de poder, ela deixou convite aberto para demais pessoas explorarem o assunto por meio da leitura, da discussão informada e do pensamento disciplinado. Na obra de 1988, ela afirma que aquele livro não é um "livro didático" convencional porque iria sugerir formas de pensamento sobre política no âmbito da economia mundial. Por esta razão, não podemos chamar suas interpretações de teoria, mas de quadro analítico (ou "framework"). Sobre isto, ela afirmou que

57 Mas não necessariamente autoridade máxima: ela pode ser máxima (por exemplo, Strange afirma que o Estado é autoridade máxima na estrutura de segurança) ou ocupar posição abaixo da máxima (um mafioso é autoridade no bairro que reside quando provê segurança aos moradores em troca de seu silêncio).

> 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 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).

Enquanto leitora e aluna de Strange, suas obras estimularam-me a pensar na possibilidade de operacionalização do conceito de difusão de poder. Além disso, senti que não haveria incoerência em buscar, dentro de sua literatura, pistas que pudessem auxiliar-me no aprofundamento da EPI e na tentativa de operacionalização do fenômeno – visto que ela própria, enquanto professora e autora, abre o convite e estimula estas atividades. Por este motivo, depois de analisar seu texto e refletir sobre as concepções apresentadas por ela, acredito que a difusão de poder opera em três dimensões – as quais chamei de "autoridade", "controle" e "resultados".[58] Estas três dimensões são fundamentadas na própria literatura de Strange (1988, 1996), de modo que, no processo de operacionalização do fenômeno da difusão, estas três dimensões puderam ser compreendidas como "variáveis qualitativas discretas" e, por isto, capazes de receberem valores numéricos.

A próxima seção do capítulo está dividida da seguinte forma: (1) buscamos fundamentar, a partir da literatura, as razões que nos levam acreditar que a difusão de poder opera em três dimensões – com destaque para trechos das obras que permitem esta reflexão; (2) apresentar as "valorações" de cada dimensão quando traduzidas para "variáveis" – ou seja, que valores são receptíveis por cada uma das três variáveis e porquê.

58 Estas palavras são as traduções respectivas de "authority", "control" e "outcomes" – palavras utilizadas por Strange no contexto de suas duas obras.

2.7.1 Dimensão "Autoridade"

Quando o leitor faz uma leitura atenta das duas obras de Strange mencionadas nesta dissertação, ele tem a capacidade de observar que três elementos encontram-se muito próximos do cerne do fenômeno de difusão de poder – e que, como se sabe, abriu caminho para as análises do SI a partir do campo da EPI. Estes três elementos são autoridade, controle e resultados.

A a**utoridade** é um conceito cuja definição é bastante complicada, como admitido pela própria britânica. No entanto, podemos afirmar que, em *The Retreat of the State*, em praticamente todas as afirmações sobre "difusão de poder", Strange utilizou o termo "difusão de autoridade" – como se fossem termos sinônimos e intercambiáveis entre si. Nossa interpretação é de que não são.

O termo "autoridade" tem, a nosso ver, duas interpretações que, apesar de serem bastante sutis, são suficientes para distingui-las: o uso do termo "autoridade" ora descreve entidade que reúne a confiança de seus pares e interessados (**ser autoridade**), ora descreve o exercício do poder (**exercer autoridade**). Acreditamos que a expressão "difusão de autoridade" (que Strange utilizou em sua obra como sendo quase sinônimo de "difusão de poder") está vinculada à segunda interpretação, que é a difusão do *exercício de poder* (exercer autoridade). Isto porque caso se referisse à difusão do "ser" autoridade isso seria traduzido no "desmembramento" do Estado, enquanto autoridade, em diversas outras entidades com menor autoridade. Ou seja, a difusão de autoridade, neste caso, significaria o surgimento de uma pluralidade de autoridades menores, originadas a partir do Estado e desvinculadas dele. E não é disto que trata o fenômeno da difusão de poder.[59]

Ser uma **autoridade** dentro do SI, visto a partir das quatro estruturas primárias, demonstra que o ator reuniu autoridade suficiente para exercê-la de modo a afetar os resultados. Assumimos que essa reunião de autoridade é outorgada pelos pares e interessados de dois modos: via consentimento ou subordinação. Uma autoridade dentro da estrutura da segurança é o Estado. Seus pares (demais Estados) e

59 Nós destacamos os trechos em que Strange (1996) versa sobre "autoridade" e reunimos em dois grupos: trechos que apresentam a autoridade como o exercício do poder; e trechos em que apresenta a autoridade como instituição, como "ser" uma autoridade. Estes dois grupos podem ser visto na lista de apêndices. Recomendamos verificar "Apêndice 1 – Ser Autoridade" e "Apêndice 2 – Exercer Autoridade".

interessados (seus nacionais) outorgam-lhe a autoridade, de modo formal, para que o mesmo seja reconhecido como soberano no SI e, assim, fluem as políticas e acordos que derivam do reconhecimento da soberania. Outra autoridade dentro da estrutura da segurança é a máfia italiana, ilustrada por Strange (1996) a partir da organização "Cosa Nostra". Esta organização é reconhecida pelos seus pares (outros grupos mafiosos) como autoridade. Cidadãos que são diretamente afetados pelas atividades desta organização (por exemplo, habitantes de um bairro com alta concentração de membros da "Cosa Nostra") podem não consentir com a autoridade da organização (muitos consentem), mas todos subordinam-se à esta autoridade se desejam evitar conflitos. Ambas as autoridades, "governo italiano" e "Cosa Nostra", se chocam e conflitam no cenário doméstico porque se rivalizam entre si. O Estado italiano observa a organização mafiosa como um rival à sua autoridade e os conflitos, fundamentados pela lei do Estado de Direito, acontecem. Neste exemplo, o que diferencia a autoridade da organização mafiosa e a autoridade do Estado é a formalidade. O governo italiano é a autoridade que concentra a identidade do Estado italiano por via formal – reconhecido por meio do voto democrático, ao qual se subordinam as forças armadas, demais instituições e cidadãos. Do mesmo modo, a seleção de futebol italiana durante uma copa do mundo também concentra, no âmbito esportivo, a identidade do Estado – mas de modo informal. A máfia italiana, por outro lado, é uma autoridade informal e ilegal.

Exercer **autoridade** é exercer poder. Este poder é exercido, de modo direto, pelo poder relacional, e de modo indireto, pelo poder estrutural. (STRANGE, 1996, p.91) No exemplo que demos acima, ambas as autoridades – Estadas italianas e a máfia por meio da organização "Cosa Nostra" – exercem poder porque influenciam os resultados para um conjunto de indivíduos e instituições e redefinem suas opções de escolha. O governo italiano é a autoridade política máxima dentro dos limites territoriais do Estado italiano, que detém o legítimo uso da força. A máfia, por outro lado, organiza-se por meio de estruturas que exercem influência sobre um conjunto de atividades e sobre a segurança de cidadãos, pois agem muitas vezes por coerção e violência.[60] Enquanto um é autoridade formal, o outro é autoridade

60 Strange (1996) destaca a sugestão de alguns sociólogos sobre a origem de autoridades mafiosas, afirmando que "Sociologists have argued that criminal gangs, like underground resistance movements in wartime or recalcitrant groups in prisons, tend to emerge when

informal. Mas ambos exercem autoridade, ambos exercem poder. Um dos objetivos dos estudiosos na área da EPI é "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).

Ser autoridade e exercer autoridade, embora muito semelhantes, implicam consequências distintas, porém complementares. Um ator pode reunir confiança suficiente de seus pares e interessados de modo a ser considerada uma autoridade em determinada matéria. Essa confiança pode ter sido outorgada por consentimento ou por subordinação imposta. No primeiro caso, podemos citar como exemplo uma organização internacional cujos membros são Estados. No início, um grupo de Estados outorgou autoridade suficiente, através de consentimento expresso, para que a Secretaria Geral desta organização pudesse começar suas atividades sobre uma determinada matéria. Com o passar do tempo, outros Estados, observando o funcionamento desta organização, decidem participar como membros. Todos estes Estados-membros são responsáveis por outorgar autoridade à organização, que desenvolve uma série de acordos vinculativos sobre a matéria em que é especialista (neste caso, é reconhecido como autoridade da estrutura do conhecimento), que devem ser seguidos por todos os membros.

Outro modo de reunir confiança dos pares e interessados é através da subordinação imposta. Imaginemos o que acontece nas favelas dominadas pelo narcotráfico na cidade do Rio de Janeiro. Facções distintas competem por poder e fatias do mercado das drogas. Imaginemos que a facção A detém a autoridade no morro e impõe uma série de regras para os cidadãos que vivem ali – como identificar-se toda vez que entrar e sair do bairro e não circular depois das 22h. Mesmo não consentindo com este conjunto de regras impostas pelo grupo dominante do morro, sem alternativa, os moradores reconhecem a facção A como autoridade (neste caso, na estrutura da segurança) e acatam suas regras de modo que, em contrapartida, não enfrentam violência. Neste cenário, surge a facção B que está interessada em dominar o morro e auferir lucros do mercado de venda de drogas. Inicia-se uma "guerra" entre os dois grupos cuja consequência é a vitória da facção B. A consequência disto é que, agora, ela é reconhecida como a nova autoridade no morro. Os moradores do bairro subordinam-se a este novo grupo.

---

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).

No primeiro exemplo, a autoridade foi reconhecida pelos Estados-membros sem que a organização exercesse poder de modo a afetar os resultados. Neste primeiro contexto, "ser autoridade" surge antes do "exercer autoridade". No segundo caso, as coisas mudam. A facção B "exerce autoridade", ou melhor, exerce poder de modo que afetou os resultados – eliminou a facção A e foi reconhecida como a nova autoridade do morro. O "ser" autoridade e o exercício da autoridade são momentos que se complementam – independente de qual momento veio primeiro. Exercer poder reforça a autoridade do ator em questão. No entanto, é importante ressaltar que o ator tende a perder autoridade ("ser autoridade") quando ele não é mais capaz de exercer poder de modo a afetar os resultados. Isto está no cerne da questão levantada por Strange (1996) quando a mesma afirmou que a autoridade de um ator não-estatal apenas poderia ser determinada com base nos resultados. Não adianta ser autoridade e não possuir capacidade de exercício desta autoridade através do poder – com o tempo, a confiança dos pares e interessados dilui-se e o reconhecimento como autoridade em determinada matéria se esvai.

Ainda cabem algumas considerações acerca do reconhecimento de autoridade por meio da confiança gerada pelos pares e interessados – especificamente dentro da estrutura do conhecimento. Exemplos sobre isso estão expressos na literatura de Strange (1988) em, pelo menos, três momentos. Na sociedade Hindu, a autoridade religiosa é sustentada pela crença. Esta era capaz de manter um conjunto de regras sobre a sociedade referentes a diversas atividades que variavam desde a higiene pessoal e o casamento até o consumo de alimentos por meio de dietas típicas. (STRANGE, 1988). A autoridade religiosa, representada pelos "brahmins", portanto, reunia a confiança dos pares e interessados de modo que segmentos da sociedade, voluntariamente, seguiam os preceitos determinados pela autoridade religiosa. Ressalta-se que esta autoridade encontra-se alocada, principalmente, na estrutura do conhecimento.

Em outra ocasião, discursando explicitamente sobre a estrutura do conhecimento, Strange (1988) aponta que a autoridade e o poder são conferidos àqueles que "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). O reconhecimento da autoridade dentro da estrutura do conhecimento – como, por exemplo, a autoridade de indivíduos que

fazem parte da comunidade científica – é dado pela sociedade que, em determinada medida, **confia** que estes membros têm o conhecimento por eles expresso. Um pesquisador da área da EPI, por exemplo, com título de doutor é reconhecido pela sociedade como tendo conhecimento sobre determinados assuntos desta agenda de estudos. A titulação, conferida por uma instituição educacional e reconhecida por um órgão do governo (representativo da sociedade em assuntos da educação), é a outorga da autoridade em matéria de EPI. É a partir desta outorga, desta confiança entregue à ele, que o pesquisador neste exemplo pode gozar de um conjunto de leis e prerrogativas legais específicas. Cabe ressaltar que, neste caso, a autoridade é formal.

Finalmente, em um terceiro momento, Strange (1988) comenta sobre a confiança dos pares e interessados para a formação da autoridade no âmbito da World Administering Radio Conference (WARC). Neste caso, ela considera a hipótese de que a burocracia internacional responsável pela WARC agiu segundo políticas próprias – ou seja, de modo independente da política dos Estados. Ela afirma que "[…] 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). Caso confirmada esta hipótese, pode-se afirmar que a confiança dos interessados foi um fator determinante para a legitimação da autoridade desta burocracia internacional no âmbito dos assuntos tratados pela WARC.

Estes três exemplos são importantes para a discussão desta dissertação porque legitimam que a autoridade, especialmente na estrutura do conhecimento, é conferida por meio da confiança dos pares e interessados na matéria sobre a qual a autoridade diz ter conhecimento. A percepção do grau de confiança dos pares e interessados – confiança crescente, confiança estável, confiança decrescente – incide sobre a variável "autoridade" presente no banco de dados gerado para esta pesquisa.

2.7.2 Dimensão "Controle"

Assim como a autoridade, o **controle** também é um elemento bastante relevante para a compreensão da difusão de poder.

Consideramos que "controle" é uma das três dimensões da difusão de poder. Em *States and Markets*, Strange (1988) aponta o papel do controle na formação do poder – com especial destaque para o poder estrutural, mas também apontando para o poder econômico e político, afirmando que

> Banks, by controlling credit, have economic power. Equally, we can say that people have political power if they control de 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)

Aqui podemos perceber que o controle sobre objeto relevante para o alcance de resultados desejados está no cerne do poder econômico e poder político. No caso dos bancos, o objeto é o crédito pois é o controle sobre ele que permite os bancos terem poder suficiente para influenciar os resultados no cenário econômico.[61] Igualmente, o controle sobre o aparato estatal por parte de um grupo político, por exemplo, lhe confere poder suficiente para influenciar os resultados do cenário político – pelo menos até certo ponto.

De modo similar, examinamos a relevância do controle no contexto das quatro estruturas a partir da seguinte citação de Strange (1988) sobre as fontes do poder estrutural:

> 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

61 Outro exemplo, para ilustrar o papel do controle no poder, refere-se ao controle político da India por parte da Grã-Bretanha. Este controle político permitiu que Londres pudesse extrair anualmente ouro e, assim, utilizar o controle sobre a oferta de ouro para influenciar o câmbio Libra-Rúpias e outros dispositivos da política cambial. Os fluxos de capital britânico foram essenciais para a manutenção do crescimento econômico do mundo pré-1914. (STRANGE, 1988, p.101).

> 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, grifo nosso).

Em outras palavras, a fonte do poder estrutural reside sobre o controle de objetos oriundos das estruturas primárias. Neste sentido, nossa atenção volta-se especialmente para a estrutura do conhecimento e o papel que o controle tem na formulação do poder oriundo a partir desta. Aqui, cabe lembrar, novamente, que o poder que se origina a partir desta estrutura também está condicionado ao controle dos canais por meio dos quais a informação circula e é armazenada. (STRANGE, 1988). Vejamos um exemplo sobre esta dinâmica.

Podemos imaginar uma instituição dedicada a pesquisas com animais marinhos. Todo o conhecimento produzido, por meio de pesquisa, coleta de dados, análise de amostras, apoia-se em conhecimento prévio sobre determinado assunto. Ao inferir que a baleia é um animal mamífero, e não um peixe, o pesquisador pode debruçar-se sobre análises de problemas típicos aos mamíferos como o desenvolvimento de leite nesta espécie de baleia específica, por

exemplo. Mas somente poderá fazer isso se souber que o animal é mamífero e que os mamíferos possuem glândulas mamárias. Alguém, em algum momento anterior, produziu o conhecimento de que as baleias são mamíferos que habitam os oceanos. Esta informação foi armazenada de modo que, a partir dela, novos estudos seguiram-se na sequência. Além disso, este conhecimento foi comunicado e compartilhado entre diversos membros da comunidade científica.

Agora imaginemos que, por terrível destino, uma grande catástrofe acometeu grande parte do conhecimento humano sobre animais de todas as espécies e que esta instituição dedicada a pesquisas com animais marinhos, e um punhado de cientistas, foi uma das poucas a se salvar de terrível destino. Imaginemos também que todo o conhecimento produzido e armazenado por esta instituição reside na "nuvem" – ou seja, em algum local abstrato de armazenamento de um computador servidor. Neste cenário hipotético, o pesquisador sênior desta instituição e o profissional de TI têm grande autoridade e poder estrutural porque controlam o acesso aos canais de informação – o pesquisador por ter experiência e conhecimento reconhecido pelos pares; e o profissional de TI por providenciar o acesso ao armazenamento deste conhecimento nos canais que a informação circula e é armazenada, ou seja, na nuvem e na rede digital de computadores. Ambos têm importância para a sociedade que segue adiante após a catástrofe. Igualmente outros indivíduos e entidades (como a instituição hipotética), neste cenário, poderão ter a capacidade de reunir autoridade suficiente em uma determinada matéria devido ao conhecimento que possuem – como, por exemplo, o conhecimento de sobrevivência na natureza. Pois, como disse Strange (1988), "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). Disto, podemos inferir que aqueles que controlam objetos (1) determinantes para o tipo de conhecimento que será pesquisado/descoberto, (2) do tipo que armazenam informações, (3) que formam canais de comunicação por onde o conhecimento é transferido; são objetos relevantes dentro da estrutura do conhecimento e confere aqueles de posse do seu controle com poder. Pois, "[…] 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)

Alguns exemplos sobre entidades que, em alguma medida, controlaram objetos considerados importantes na estrutura do conhecimento e galgaram poder são destaque na literatura de Strange (1996): a igreja Católica na Europa Cristã medieval; o Estado cientificista na Segunda Guerra Mundial; empresas que detêm o monopólio sobre uma tecnologia específica; entre outros casos.[62] O controle sobre determinado objeto representa poder – que, naturalmente, influencia os resultados. Por esta razão, controle é uma das dimensões da difusão de poder.

2.7.3 Dimensão "Resultados"

Os resultados compõem a terceira dimensão da difusão de poder. Ele está intimamente relacionado às dimensões autoridade e controle porque representa a existência de

efetividade de ambas. Podemos assumir que um determinado ator, no contexto da EPI, detém autoridade sobre uma matéria. Por meio desta autoridade, lhe são conferidos obediência e subordinação. Também podemos assumir que este ator detém o controle sobre um objeto considerado, por pares e interessados, relevante no cenário político-econômico. Consequentemente, este ator é considerado importante dentro do contexto da EPI. Em ambas as situações, o que atesta a autoridade do ator, e o que atesta que este detém o controle sobre o objeto, é sua capacidade de influenciar nos resultados. Ou seja, caso seja verificado, por meio dos resultados, que o ator teve capacidade de influenciar no status-quo, sua autoridade é reforçada e/ou seu controle é confirmado. Caso não seja verificado sua capacidade de influenciar os resultados, sua autoridade é abalada – o que significa que a confiança dos pares e interessados será diminuída – e/ou controle sobre determinado objeto será questionado. A dimensão "resultados" é aquela que confirma, questiona ou rejeita a efetividade do poder por parte do ator em questão. Cabe ressaltar que o poder incide sobre os resultados, por meio do status-quo, de dois modos: mantendo-o ou alterando-o.

62 Nós reunimos em uma tabela exemplos oriundos de ambas as obras de Strange (1988, 1996) que se referem ao "controle" e ao "objeto" do controle. É possível verificar que em alguns momentos ela aponta que o "controle" representa poder. Ver "Apêndice 3 – Controle, 1988" e "Apêndice 4 – Controle, 1996".

O surgimento das redes de informações baseadas na microeletrônica, da qual a rede mundial de computadores faz parte, propiciou o surgimento do domínio cibernético. A dimensão "resultados" preocupa-se com a incidência do poder sobre o status-quo no plano real, e não no plano digital. Ou seja, são os resultados que incidem sobre o plano real geográfico que são considerados relevantes para a análise de difusão de poder porque é neste plano que encontram-se os atores. Já os resultados que incidem apenas no plano digital, sem incidência alguma sobre o real, encontram-se em um sistema fechado na abstração e, por esta razão, não são relevantes para análise de difusão de poder segundo o campo da EPI. A dimensão "resultados" tem, portanto, como conteúdo principal o efeito na realidade geográfica onde se encontram os atores. Os resultados gerados no plano cibernético serão levados em consideração apenas se incidirem, também, sobre a realidade geográfica. Na introdução, apontamos o exemplo de um indivíduo participando de um jogo virtual para lazer próprio e no contexto de um campeonato.

2.74 Operacionalização das Dimensões

As três dimensões mencionadas anteriormente foram operacionalizadas de modo a tornarem-se variáveis qualitativas discretas. Cada uma das três variáveis recebem valores que variam de acordo com a dimensão, conforme explicitado na introdução desta dissertação.

A primeira variável, **autoridade**, tem como conteúdo o sentido de confiança. Este sentido diz respeito à confiança que os pares e interessados na matéria depositam na autoridade em questão. A confiança depositada (ou a falta dela) designa crescimento, manutenção ou decrescimento do **nível** de autoridade do ator sobre uma determinada matéria. Por esta razão, esta variável pode receber os valores inteiros "-1" (decrescimento), "0" (manutenção) e "+1" (crescimento).

As concepções de "crescimento", "manutenção" e "decrescimento" foram retiradas da própria literatura de Strange (1988, 1996). Na obra *States and Markets*, ela discorreu sobre essa variação gradual da autoridade. Destacamos alguns exemplos, como quando versa sobre o decrescimento da autoridade da Igreja Católica na Europa cristã medieval:

> 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)

Em outro momento, entende-se que o decrescimento da autoridade da Igreja Católica, dentro da estrutura do conhecimento – ou seja, no que diz respeito ao conhecimento produzido, armazenado e compartilhado na sociedade – foi substituído, gradativamente, pela crescente autoridade do Estado científico. Enquanto a Igreja viu seu poder reduzir, o Estado científico viu seu poder sobre a sociedade e suas atividades crescer:

> [...] 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, grifo nosso)

Depois de dominar a estrutura do conhecimento e legitimar-se como autoridade máxima na estrutura do conhecimento, o Estado científico "lutou" pela **manutenção** do seu nível de autoridade – como podemos ver neste trecho destacado por 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, grifo nosso).

Em outra ocasião, Strange (1988) explica tanto o **declínio** da autoridade do governo norte-americano sobre corporações transnacionais com sede nos EUA, quanto seu **crescimento** sobre corporações transnacionais estrangeiras que operam no território norte-americano:

> 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, grifo nosso).

Já na obra *The Retreat of the State*, 1996, em que discorre sobre a difusão de poder propriamente dita, seu argumento central é relativo ao declínio da *qualidade* da autoridade dos governos da maioria dos Estados territoriais – e não sobre o declínio da *quantidade* do exercício da autoridade. (STRANGE, 1996). Seja como for, sua tese central respalda-se sobre a diminuição da autoridade dos Estados sobre pessoas

e atividades dentro de seus territórios, não a substituição da autoridade do Estado por outras autoridades não-estatais. A existência de outras autoridades não-estatais ora competem, ora rivalizam com a autoridade estatal nas quatro estruturas primárias definidas pela EPI de Susan Strange.

Ao discutir a rivalidade entre as autoridades do Estado italiano e da organização mafiosa "Cosa Nostra", Strange (1996) aponta que o relacionamento entre ambos se tornava instável em duas ocasiões: ou quando a autoridade de qualquer uma das partes enfraquecia-se, ou quando a autoridade de uma das partes tornava-se forte o suficiente a ponto de ameaçar a outra. Ela afirmou que

> 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, grifo nosso)

Finalmente, ela reforça a ideia de aumento, manutenção e declínio de autoridade quando discute o papel de determinadas profissões no cenário global da economia política, como os gerentes do negócio de seguros:

> 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, grifo nosso)

Tendo em vista que Strange (1988, 1996), em diversas ocasiões discutiu sobre autoridade, *e flutuações da autoridade*, nós acreditamos que "crescimento", "manutenção" e "declínio" de autoridade incidem sobre a balança de poder.[63] A variável "autoridade" representa uma das dimensões da difusão de poder.

A segunda variável, **controle**, tem como conteúdo o sentido de exercício ou operação de um determinado objeto por um ator. O controle de objetos pode ser absoluto, parcial e nenhum. Ele é absoluto quando o ator em questão é o único responsável pelo controle de determinado objeto, direcionando-o da forma como deseja. É parcial quando não é o único responsável pelo controle do objeto, ou quando depende de outros atores para controlar o objeto. E não tem controle algum quando não é o responsável pelo controle do objeto, ou quando não tem acesso ao objeto.

Um exemplo clássico do papel do controle na literatura de Strange (1988) trata sobre o poder que a burocracia tem sobre o objeto produzido por produtores e consumido por consumidores – o que afeta, diretamente, a produção e a economia de um mercado doméstico, por exemplo. Ela afirmou que

> 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)

Os incentivos que o Estado fornece aos produtores, de modo que estes produzam quantidade suficiente para atender o mercado de consumidores, deve ser de tal modo que a falta do produto não incida sobre a economia, afinal, os produtores têm o controle absoluto sobre o produto – não o Estado. Este último, indiretamente, faz uso de incentivos para incidir sobre a produção. Seu controle sobre o produto é parcial.

63 Entende-se por balança de poder o jogo de forças, de poder entre atores estatais e não-estatais no SI. Não deve ser compreendido como a expressão clássica utilizada no Realismo.

Outro exemplo discorre sobre empresas multinacionais que sofrem apropriação por parte do Estado. Embora estas empresas sejam recompensadas, como manda a lei internacional, o Estado, muitas vezes, depara-se com frustrações: os Estados, neste caso, detêm a produção, o maquinário, os recursos para explorar o mercado, mas não a tecnologia, conhecimento e acesso ao mercado. Afinal, o acesso ao mercado permanece sob o controle das antigas empresas desapropriadas. São elas que detêm o controle sobre tecnologia, conhecimento e acesso ao mercado. E este controle significa poder. Em especial, Strange (1988) cita os casos da Nigéria e do Chile, afirmando que estes países

> 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, grifo nosso)

No caso da estrutura do conhecimento, a Igreja Católica teve seu poder e autoridade reforçados pelo controle sobre os meios de comunicação (livros sagrados, alfabetização no idioma do Latin – oficial dentro dos ritos religiosos). (STRANGE, 1988). Para Strange (1988), é o controle sobre o acesso ao conhecimento que propiciou a manutenção do poder com a Igreja Católica – o que indica que autoridades rivais dentro desta estrutura tiveram que ser eliminadas ou descreditadas. (STRANGE, 1988, p.124). O controle da Igreja Católica na Europa Cristã Medieval sobre o conhecimento foi, por vezes, absoluto. O enfraquecimento da autoridade da Igreja na estrutura do conhecimento, frente a crescente autoridade do Estado científico, trouxe à tona a relevância da ciência e da comunidade científica. O eixo da autoridade máxima dentro da estrutura do conhecimento deslocou-se da Igreja para o Estado. As escrituras sagradas, o idioma Latim foram substituídos pelo

cientificismo e pela língua inglesa. A crença, por parte dos pares e interessados (sociedade em geral e governos nacionais, principalmente), na Ciência (e na comunidade científica, por consequência) como autoridade sobre fatos naturais significou a erosão da autoridade da Igreja sobre a mesma matéria – relegando esta às questões espirituais e da fé humana. (STRANGE, 1988). Neste contexto, o controle da Igreja sobre os meios de comunicação não permaneceu com a mesma relevância: correios, telégrafos e telefone – oriundos a partir de descobertas da comunidade científica e controlados por Estados e empresas privadas – significaram poder àqueles que detinham seu controle. Em outras palavras, os objetos relevantes para o alcance dos resultados desejados, dentro da estrutura do conhecimento, se alteraram e significaram poder para quem tivesse o controle destes novos objetos.

Em outra ocasião, Strange (1996) cita o monopólio do controle por empresas sobre uma tecnologia, suprimento, ou sistema de marketing, ou mesmo marca. No mercado global, este monopólio significa poder sobre o conjunto de atividades do setor e consumidores interessados nos produtos específicos desta empresa. Com o tempo, pode ser que a tecnologia se torne compartilhada (engenharia reversa é uma das ferramentas mais utilizadas) e o poder que advém do controle seja, pouco a pouco, erodido – até que uma nova tecnologia seja desenvolvida e o monopólio sobre ela seja implantado. Ou, como no caso de cartéis que controlam o suprimento de diamantes do mundo: seu poder deriva do controle rígido, quase absoluto, sobre os suprimentos. De acordo com 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).

Existem outros exemplos de controle sobre um objeto, seja ele de total, parcial ou nenhum. Sugerimos verificar “Apêndice 3 – Controle, 1988” e “Apêndice 4 – Controle, 1996”.

Finalmente, sobre a variável “resultados”. Existem apenas dois tipos de resultados: aqueles que alteram o status-quo; e aqueles que não o alteram. A alteração do status-quo (da situação atual das coisas, ou

melhor, o estado atual de algo) significa uma mudança de estado. Alterar o status-quo implica em substituição de uma situação por outra diferente. Já a não-alteração do status-quo implica em sua permanência, seu reforço. Em outras palavras, existe um combate entre forças para alteração ou permanência do status-quo. Não existe alternativa além destas duas. Cabe apenas lembrar que o status-quo refere-se à região onde se encontram os atores, ou seja, o plano real geográfico (e não na abstração dos sistemas de informação como o domínio cibernético).

2.8 O PODER NO DOMÍNIO CIBERNÉTICO

Nesta seção, faremos breves considerações sobre o poder no domínio cibernético a partir de dois expoentes da área de Relações Internacionais: Susan Strange e Joseph Nye Jr.

Primeiro, e antes de tudo, é preciso estabelecer que as duas obras de Strange utilizadas nesta pesquisa, *States and Markets*, 1988, e *The Retreat of the State*, 1996, não apontam indícios da EPI no contexto específico da Internet. Em 1988, a Internet ainda não havia sido comercializada.[64] Em 1996, uma pequena parte da população mundial dava seus primeiros passos na rede mundial de computadores. Os estudos acerca dos fenômenos oriundos do novo domínio cibernético eram poucos. Contudo, mesmo que não tenha discutido especificamente a EPI no contexto da rede mundial de computadores, Strange elucida pontos de discussão interessantes sobre as alterações tecnológicas e os sistemas da informação a partir da estrutura do conhecimento. Nós destacamos alguns pontos que acreditamos serão capazes de fornecer bases suficientes para considerar o estudo da EPI no domínio cibernético – essência da presente pesquisa.

Segundo, optamos por apresentar um pouco sobre os estudos recentes de Joseph Nye em razão de suas considerações cibernéticas e por discutir "difusão de poder" e "transição de poder" no seu trabalho – mesmo que sua discussão sobre "difusão de poder" não seja relacionada com a discussão que Strange realiza. Nye talvez seja o maior expoente da área de RI a realizar considerações sobre a disciplina no domínio cibernético.

64 De acordo com Ceruzzi (2003, p.321), a internet se comercializou, nos Estados Unidos, no ano de 1995.

2.8.1 Susan Strange: Inovações Tecnológicas, Sistemas de Informação e Difusão de Poder na Estrutura do Conhecimento

Na obra *The Retreat of the State*, Strange (1996) argumenta que estavam sendo desenvolvidos, no final do século XX, proposições gerais sobre a autoridade no contexto da EPI. Uma destas proposições afirmava que a autoridade do governo de todos os Estados têm enfraquecido como resultado de mudanças tecnológicas, financeiras e da integração acelerada das economias nacionais em uma economia de mercado global único. Para nós, é relevante apontar o papel tecnológico neste cenário de final de século que, segundo ela, é bastante negligenciado pela academia – muito embora seja de extrema importância para a consolidação desta nova dinâmica. Sobre isto, Strange afirma que

> 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, além de reconhecer o fator tecnológico como causa essencial das alterações da balança de poder, indica que é o elemento capaz de explicar mudanças tanto econômicas quanto políticas. E as novas tecnologias da informação – provenientes de conhecimentos e descobertas específicas – representadas em larga medida pela Internet, têm grande responsabilidade nisso. O conhecimento necessário para a criação destes novos sistemas conferiu autoridade a grupos de cientistas específicos dentro da estrutura do conhecimento. Da mesma forma, as

demais estruturas (segurança, produção e finanças) tiveram, em menor ou maior grau, incidência sobre o desenvolvimento da Internet.

Pela ótica da estrutura da segurança podemos perceber a preocupação de setores militares das forças armadas norte-americanas em criar um sistema de comunicação capaz de resistir a ataques nucleares. Pela estrutura da produção, fabricantes de peças de computador tiveram que entrar em consenso no que diz respeito ao design e tecnologias implementadas no hardware de modo que "permitissem" a padronização do acesso a rede mundial. A harmonização da produção de máquinas e peças propiciou a compra em massa de computadores com capacidade de atender aos pré-requisitos de hardware e software para se conectarem a Internet. Pela estrutura das finanças, observamos que a abertura comercial da Internet impulsionou a indústria de softwares e plataformas digitais, capazes de movimentar o mercado financeiro e ganhar autoridade no setor da computação.[65]

Em suma, a Internet é fruto de três forças complementares na segunda metade do século XX – Big Data[66], militares e comunidade científica. [67] Ao final deste século, os Estados, as empresas e parte da população civil tiveram acesso à Internet comercial e adentraram o domínio cibernético. Se é verdade que os limites geográficos não mais coincidem com a extensão da autoridade política sobre a economia e a sociedade, como afirma Strange (1996), é razoável supor que esta autoridade busca legitimar-se dentro do domínio do ciberespaço – onde fluem as comunicações, as trocas de serviço e nascem novas tecnologias de software provenientes do conhecimento – afinal, "a sociedade em rede" é uma nova dimensão da própria sociedade.[68]

---

65 Informações acerca da origem da Internet são discutidas em mais detalhes no capítulo 2 desta dissertação.

66 Para Schatz (2014), a "Big Science" não foi resultado de eventos específicos como o "Manhattan Project" ou o "Apollo Programe", mas desenvolveu-se gradualmente da "Little Science". Para Hallonsten (2014), uma das manifestações entre a ciência e o Estado é a "Big Science", que se encontra no eixo entre a ciência fundamental e as pesquisas e desenvolvimentos militares.

67 De acordo com Castells (2001, p.17) a Internet foi uma descoberta proveniente da intersecção entre a Big Science, a pesquisa militar e a cultura da liberdade. A primeira, desenvolvida pelos norte-americanos ao longo do século XX; a segunda é evidência de que o setor militar é, também, motor propulsor de inovações tecnológicas provenientes de pesquisa e desenvolvimento próprios; e a terceira, demonstra a participação do setor civil por meio dos acadêmicos universitários que estimularam o crescimento da rede mundial.

68 Sobre isso, os estudos de Castells (2005) são relevantes. Para o autor, o mundo está em processo de transformação estrutural multidimensional associado à emergência de um novo paradigma tecnológico. Esta sociedade emergente, caracterizada como sociedade de informação ou sociedade do conhecimento, é diferente das demais sociedades que já

Vale lembrar que a Internet é um regime híbrido composto por aspectos físicos e digitais. (LIBICKI, 2009). Ela funciona a partir de uma teia de infraestrutura de telecomunicações que se distribui verdadeiramente pelo globo terrestre. (CANABARRO, 2014, p.26). Além da estrutura física de cabos, satélites, modens, roteadores, etc., ela responde a uma estrutura digital, onde se encontram os protocolos, os endereçamentos, o roteamento de pacotes, softwares, etc. De acordo com Canabarro (2014), "a Era Digital diz respeito basicamente à manipulação, armazenamento e propagação de informações em formato digital através de dispositivos eletrônicos, o que permitiu o desenvolvimento da computação digital." (CANABARRO, 2014, p.26). O ponto é que quando se discute o desenvolvimento da Internet, discute-se tanto o aspecto físico, quanto o aspecto abstrato das ideias que impulsionam as inovações digitais e tecnológicas. A estrutura do conhecimento contribuiu em larga medida para a criação da Internet. Tudo isto evidencia fundamentos para a existência do poder estrutural neste novo paradigma tecnológico. Ressaltamos que a própria Strange (1988) apontou, ao final da década de 1980, que os Estados estavam cientes da importância dos recursos intangíveis que se originam a partir de uma forte sociedade civil. Para eles, estes recursos intangíveis poderiam, inclusive, compensar deficiências da nação como tamanho da população e território ou força bélica.[69]

Outro ponto importante é que Strange (1988) deu indicativos do que seria considerado como conhecimento importante para a estrutura do conhecimento. Este conhecimento deveria tratar, especialmente, sobre (1) qualquer mudança no fornecimento, ou no controle, da informação e dos sistemas que abarcam a comunicação no geral; (2)

---

existiram por "serem de base microelectrónica, através de redes tecnológicas que fornecem novas capacidades a uma velha forma de organização social: as redes". (Ibid., p.17). Nesse sentido, o autor considera que a nova "sociedade em rede" é potencializada pela mais "extraordinária revolução tecnológica da humanidade, que é capaz de transformar as nossas capacidades de comunicação, que permite a alteração dos nossos códigos de vida, que nos fornece ferramentas para realmente controlarmos as nossas próprias condições, com todo o seu potencial destrutivo e todas as implicações da sua capacidade criativa. […] O que nós sabemos é que esse paradigma tecnológico tem capacidades de performance superiores em relação aos anteriores sistemas tecnológicos." (Ibid., p.19). Dessa forma, conclui-se que "a comunicação em rede transcende fronteiras, a sociedade em rede é global, é baseada em redes globais. Então sua lógica chega a países de todo o planeta e difunde-se através do poder integrado nas redes globais de capital, bens, serviços, comunicação, informação, ciência e tecnologia." (Ibid., p.18)

69 Alguns Estados, inclusive, também incluem nesta seara o controle sobre os sistemas de comunicação, os sistemas de transporte aéreo e marítimo, e o comando de habilidades técnicas, por exemplo. (Ibid., p.38)

alterações que pudessem incidir sobre a utilização do idioma ou sobre canais não-verbais de comunicação; (3) e também mudanças de percepção considerada fundamentais sobre a condição humana que pudessem influenciar julgamentos de valor. Por meio destes indicativos, podemos considerar que a Internet é marco relevante dentro da estrutura do conhecimento.

Embora não tenha versado sobre a Internet, ao final da década de 1980 Strange demonstrava estar consciente das mudanças tecnológicas em curso na sociedade, uma vez que destacou em sua obra duas inovações técnicas que considerava especialmente centrais ao debate que se apresentava naquele período. A primeira inovação se referia ao desenvolvimento de computadores sofisticados; e a segunda inovação dizia respeito as comunicações eletrônicas por meio de satélites. Estas duas inovações, segundo ela, foram responsáveis por resultados imediatos: unificaram os mercados nacionais sobre todos os produtos e serviços. (STRANGE, 1988). Estas declarações sobre inovações tecnológicas são relevantes pois demonstram que, mesmo que não tenha discutido a Internet, Strange não estava "adormecida" sobre os acontecimentos desenrolados ao final da década de 1980 e 1990 que culminaram com a ascensão da rede mundial de computadores. O seu esforço analítico sobre os sistemas da informação e as inovações tecnológicas dos computadores, embora breve, residiu, essencialmente, sobre a estrutura do conhecimento. E considerava a existência de desenvolvimentos, oriundos da estrutura do conhecimento, demasiado importantes para a EPI – uma vez que a competição entre os Estados, naquela época, podia ser lida como competição pela liderança tecnológica.[70] Sobre isso, ela expôs que

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

70 Embora os resultados ou conclusões destes desenvolvimentos à sua época não serem claros, ela argumentou que existiam evidências suficientes para sustentar esta afirmação. (STRANGE, 1988, p.136)

> 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)

Ao final da década de 1980, a autora percebe as transformações tecnológicas e o impacto político dentro da estrutura do conhecimento – forte suficiente para destacar a importância de análises por meio do campo da EPI. As transformações oriundas da transição da sociedade em rede para a base microeletrônica, conforme mencionado por Castells e Cardoso (2005), aliadas a outras alterações tecnológicas em setores diversos, parecem levar Strange a concluir que, de fato, esta é a estrutura que está passando por mudanças mais rápidas, mesmo que seja a estrutura primária mais negligenciada. (STRANGE, 1988). É neste contexto que ela destaca que as preocupações dos estudiosos em EPI devem voltar-se para *a natureza do poder exercido por meio da estrutura do conhecimento*; e para os centros de poder – questionando se estes centros estão passando por alterações significativas. (STRANGE, 1988, 136).

Partindo do que foi discutido até aqui, tudo indica que não há motivos para desconsiderar a análise da EPI no contexto da Internet – uma vez que é um espaço onde produtos e serviços são comercializados, agentes trocam informações e partilham conhecimento, novas tecnologias abstratas são desenvolvidas e implementadas como novos sistemas de comunicação não-verbal. Em suma, se é verdade que a EPI estuda os desenvolvimentos políticos e econômicos de modo complementares, acompanhando assim a sociedade, não há razão para supor que ela não deva estar presente na nova dimensão da sociedade: aquela sedimentada em rede e fundamentada a partir da base microeletrônica – o ciberespaço.

2.8.2 Joseph Nye Jr.: Cyberpower, Difusão e Transição de Poder

O norte-americano Joseph Nye Jr. é conhecido, especialmente, por suas formulações sobre Poder Brando ("soft power") e Poder Duro ("Hard Power"). Em 2011, ele lançou a obra *The Future of Power*, em que descreve a mais nova modalidade de poder no século XXI: *Cyberpower* ("Poder Cibernético"). Um ano antes, Nye já afirmava que o "cyberspace is a new and important domain of power." (NYE, 2010, p.2). Ele também definiu o Poder Cibernético:

> 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 admite que o Poder Cibernético relaciona-se, também, a um conjunto de recursos. Estes recursos não são tangíveis, uma vez que estão relacionados com a criação, controle e comunicação de informações baseadas na dimensão da eletrônica e dos computadores. Ou seja, o Poder Cibernético, dito por Nye (2011) como representativo do poder próprio do século XXI, parece corresponder ao tipo de poder estrutural oriundo, principalmente, da estrutura do conhecimento de Susan Strange (1988) – com a única diferença de ser um tipo de poder existente exclusivamente no domínio do ciberespaço.

Podemos correlacionar o trecho destacado acima às obras de Strange sobre poder estrutural e difusão de poder. Neste sentido, identificamos a dualidade do Poder Cibernético: tal qual o poder exercido no SI segundo o campo da EPI, ele também parece estar associado ao poder relacional e estrutural. Diretamente, o Poder Cibernético é exercido através do poder relacional – pois reflete as habilidades de obterem-se os resultados desejados. Indiretamente, o Poder Cibernético é exercido através do poder estrutural porque seu cerne está fundamentado no conjunto de recursos que se relacionam com a criação, controle e comunicação de informações – ou melhor,

conhecimento. Tal como Strange (1988), que observa o poder no SI sob essas duas vertentes, o Poder Cibernético de Nye (2011) também apresenta esta dualidade.

É interessante notar como Nye (2011) admite que o ciberespaço é, de fato, um novo domínio do poder – que se inicia ao final do século XX. Segundo ele, pelo fato de ser um domínio em si, esta nova arena requer a atenção especial de intelectuais e estudiosos de RI, se os mesmos desejam compreender o cenário da política internacional no século XXI de modo mais abrangente. Esta atenção é necessária pois, de acordo com ele "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). Como percebido, Nye (2011) também discorre sobre a difusão de poder. No entanto, diferentemente de Strange (1996), ele não utiliza o contexto das estruturas primárias para fundamentar o fenômeno da difusão de poder no ciberespaço.

Na obra *The Future of Power*, Nye (2011) admite que dois tipos de deslocamentos de poder estão ocorrendo no século XXI: transição de poder e difusão de poder. No primeiro caso, a transição de poder refere-se ao deslocamento de poder no sentido horizontal – ou seja, de um Estado dominante para outro Estado. Este processo é considerado familiar pela literatura de RI e é evidenciado pelos estudos da História. No caso do novo milênio, refere-se especialmente ao deslocamento do eixo de poder do Ocidente para o Oriente. (NYE, 2011). Já a difusão de poder, segundo ele, seria um processo novo e recente que designa um deslocamento de poder no sentido vertical – que fundamenta a relevância de novos atores (não-estatais) no SI.

De acordo com ele, quando se trata do ciberespaço, observa-se que um dos fatores que contribui para a difusão de poder é uma parte das atividades que ocorrem neste domínio estão fora do alcance do Estado. Ou melhor, fora do seu **controle**. (NYE, 2011). O surgimento de novos atores, aliado à falta de controle do Estado, proporciona a difusão de poder no ciberespaço. Este surgimento massivo de uma miríade de atores torna-se possível através da redução do custo da transmissão de informação. A tecnologia rapidamente perde seu valor de custo. Os novos atores no domínio cibernético, segundo ele, competem por poder e desafiam o Estado. É por esta razão que Nye (2011) acredita que a centralidade da rede seja a dimensão-chave do poder no século XXI.[71]

71 Se correlacionarmos com os estudos liderados por Strange (1988, 1996) poderíamos afirmar que os atores capazes de competir por poder neste novo domínio representam autoridades na estrutura do conhecimento. Suas habilidades no domínio cibernético ora

Mas, de que modo a ascensão de diversos atores na rede mundial de computadores contribui para a difusão de poder? Da seguinte forma: o aumento elevado do número de usuários com acesso à rede mundial é explicado pela redução do custo de entrada ao ciberespaço. Este novo domínio tem características inerentes que são capazes de promover o que Nye chama de "redução dos diferenciais de poder". (NYE, 2011, p.150, tradução nossa). O raciocínio é relativamente simples: o domínio do ciberespaço é extremamente novo quando comparado aos domínios de terra, mar e ar. E nestes domínios, nem todas as "peças" possuem "cartas suficientes" para iniciar o jogo do poder. O ciberespaço, ao contrário destes domínios, e devido ao seu reduzido custo de acesso, proporciona a entrada de diferentes "peças" com "cartas suficientes" para iniciar o jogo do poder. Nye, inclusive, apresenta alguns alvos do poder no domínio do ciberespaço – verificar "Anexo 2 – Dimensões Físicas e Virtuais do Poder Cibernético".

De modo resumido, podemos dizer que o baixo custo de entrada ao ciberespaço – que caracteriza o surgimento de novos atores – somado às características inerentes deste domínio são responsáveis por promover a redução dos diferenciais de poder entre os atores. No domínio cibernético, o poder entre os diferentes atores tendem a equalizar-se. Afinal, "ataques de negação de serviço distribuído" – conhecidos como ataques "DDoS" (sigla para "Distributed Denial of Service Attacks"), um instrumento de poder nesta área, por exemplo – podem ser lançados por qualquer indivíduo na rede – Estados, empresas, indivíduos, organizações, etc, *desde que tenham conhecimento*. Atores diferentes possuem recursos de poder diferentes no ciberespaço. A lacuna que separa atores estatais e não-estatais se estreita em muitas instâncias. Este estreitamento é o diferencial deste novo domínio.[72] (NYE, 2011).

Finalmente, duas observações. Primeiro, para Nye (2011), difusão de poder e equalização de poder não são o mesmo fenômeno. Segundo, Nye (2011) reconhece que "although cyberspace may create some power shifts among states by opening limited opportunities for leapfrogging by

---

rivalizam e desafiam o poder do Estado (em manter as atividades e indivíduos subordinados à sua autoridade), ora reforçam o poder do Estado quando alia-se à ele.

72 Aqui, vale a pena lembrar que o desenvolvimento de tecnologias de software não estão circunscritas as universidades de computação ou empresas do setor tecnológico. Qualquer indivíduo com acesso à Internet, e conhecimento suficiente, pode desenvolver programas de computador, aplicativos, softwares que serão utilizados por outros atores na rede ou fora dela. Considero esta uma grande evidência da estrutura do conhecimento no domínio do ciberespaço.

small states using asymmetrical warfare, it is unlikely to be a game changer in the power transitions […].” (NYE, 2011, p.151).

As alterações nos sistemas de informação e as recentes inovações no campo computacional foram apontadas por Strange (1988) como relevantes e merecidas de análise por parte da EPI – ainda na década de 1980. Mais de 20 anos depois, Nye (2011) aponta que a difusão de poder no ciberespaço evidencia que o novo domínio cibernético é dimensão-chave para a compreensão do poder pela disciplina de RI no século XXI.

2.9 CONCLUSÃO

O objetivo deste capítulo inicial foi apresentar o marco teórico adotado por esta pesquisa: a EPI a partir da britânica Susan Strange. Em especial, nos interessa a discussão teórica em torno do fenômeno “difusão de poder” – tendo em vista que a pesquisa busca compreender como, e em que medida, a rede TOR aumenta a difusão de poder no século XXI.

Para isto, apresentamos as duas principais abordagens sobre o poder na área das Relações Internacionais. A intenção foi apontar a “ruptura” conceitual, entre Strange e as correntes teóricas tradicionais em RI, que resultou na emergência da noção de poder estrutural. Esta emergência foi responsável por inaugurar a disciplina da EPI – responsável, em larga medida, por unir as áreas da Política e da Economia em uma visão global de mercados e Estados. É a partir disto que Strange explicita o fenômeno da difusão de poder.

Outro estudioso da área das Relações Internacionais que versou sobre “difusão de poder” foi Joseph Nye Jr. Diferentemente de Strange, Nye teve a oportunidade de realizar considerações específicas sobre o que chamou de “novo domínio do poder”: a região do ciberespaço. Talvez por esta razão, ele siga atualmente como referência dentro da área no que diz respeito estudos envolvendo a Informática e as Relações Internacionais. A discussão em torno do trabalho recente do norte-americano, nesta pesquisa, aconteceu por duas razões: primeiro, pretendíamos apontar as diferenças e semelhanças entre o conceito de “difusão de poder” entre Nye e Strange; segundo, apresentar, brevemente, seu estudo teórico acerca do domínio cibernético.

De modo resumido, o conceito de "difusão de poder" de Strange se assenta sobre as estruturas primárias, as quais permitem espaço para que atores não-estatais tenham poder. Este poder foi definido por ela como "poder estrutural". O conceito de "difusão de poder" de Nye, no entanto, não discute (pelo menos explicitamente) as estruturas primárias: seu trabalho aponta a difusão de poder fomentada pelo surgimento de atores não-estatais no domínio cibernético (através da redução dos custos de entrada a este domínio) e às tecnologias próprias do ciberespaço.[73] Estes atores, por vezes, têm poder suficiente para alcançar resultados desejados através dos recursos inerentes do ciberespaço. Para ele, estes resultados podem ocorrer dentro ou fora deste domínio. Enquanto No entanto, apesar de partirem de diferentes epistemologias, ambos fenômenos de difusão de poder têm similaridades: a difusão de poder, de Nye ou Strange, ocorre no sentido "vertical" – de Estados para atores não-estatais.

Neste capítulo também fundamentamos nosso ponto de partida acerca da operacionalização do fenômeno da difusão de poder segundo Strange (1996). Em especial, destacamos o papel das variáveis na compreensão das dimensões da difusão de poder. Estas dimensões são três: autoridade, controle e resultados.

73 Segundo Nye (2011), este domínio detém características inerentes que permitem a "redução dos diferenciais de poder" entre os diversos atores que nele realizam atividades.

3. CAPÍTULO 2: DARK WEB E REDE ANÔNIMA TOR

A Dark Web, por meio da rede anônima The Onion Router (TOR), é o ambiente no qual esta dissertação busca analisar a difusão de poder. A rede TOR é uma das redes que compõem a Dark Web, juntamente com demais redes que realizam um esforço ativo de blindagem das comunicações, como a rede Freenet e a rede I2P. De modo específico, o conhecimento técnico da rede TOR e, de modo geral, das políticas em torno do anonimato conferido por este canal de comunicação são essenciais para a análise da difusão de poder. Sendo assim, este capítulo fundamenta as razões pelas quais acreditamos que a Dark Web seja o ambiente dentro do domínio cibernético que mais desafia a autoridade do Estado e emana graus de poder a diversos atores – sejam eles atores públicos ou privados.

Nós dividimos este segundo capítulo em três grandes partes: a primeira parte refere-se aos assuntos necessários para definir e contextualizar a Dark Web no universo da World Wide Web (WWW), parte do ciberespaço; a segunda parte busca, no contexto da Dark Web, apresentar a rede anônima TOR em seu aspecto técnico e político; a terceira parte fundamenta a rede anônima TOR como parte relevante da estrutura do conhecimento no século XXI.

Na primeira parte, nós iniciaremos com o histórico da rede mundial de computadores, sua origem e funcionamento técnico. Com isso, nós buscamos mostrar pontos fundamentais para que dispositivos eletrônicos operem na malha da Internet – como os protocolos e a comutação de pacotes. O protocolo TCP/IP, por exemplo, foi responsável por estabelecer conexões entre computadores distintos, criando o sistema de redes de informação digital. A comutação de pacotes se refere ao endereçamento estratégico dos dados que navegam na rede. Todavia, é bastante comum que indivíduos utilizem diferentes termos técnicos para designar a mesma coisa no âmbito da rede mundial de computadores. Por exemplo, Finklea (2005) aponta que usuários utilizam o termo “world wide web” como sinônimo de “internet”, embora não o sejam. Para que isso não ocorra, sentimos a necessidade de explicar, além do histórico da Internet, diferentes termos técnicos como “rede”, “Internet”, “WWW”, “Surface Web”, “Deep Web”, “Dark Web” e “TOR” – além de protocolos e comutação de paccotes. Todos esses termos estão, em algum sentido, relacionados entre si.

Em seguida, apresentaremos a WWW, comumente conhecida por "web". A WWW é uma das camadas de aplicação que opera através da Internet. E nesta camada, segundo classificação atual, existem seis diferentes categorias na Web: Surface Web, Opaque Web, Private Web, Proprietary Web, Truly Invisible Web e Dark Web. A Surface Web é a navegação convencional da WWW (utilizando *browsers* como Google Chrome, Mozilla Firefox, Safari, Opera, etc) por meio dos portais de busca como "Google", "Yahoo" e "Bing!". Diferente da Surface Web, a Deep Web é composta pelas outras cinco categorias – cujo conteúdo não é indexado pelos motores de busca dos portais supracitados, ou seja, não serão apresentados numa lista como resultados.

A segunda parte visa apresentar a rede anônima específica para fins de análise desta pesquisa – The Onion Router (TOR). Segundo Finklea (2015), a rede TOR, das redes anônimas que compõem a Dark Web, é a maior em número de usuários e conteúdo armazenado. Nós explicitaremos sua origem, a técnica do "roteamento cebola" – responsável por encriptar mensagens e ocultar a identidade dos usuários –, as "Tor Bridges", que auxiliam nas atividades contra-censura; os serviços ocultos inerentes à rede, sua popularidade e seu aspecto político. Nosso objetivo foi explicitar os aspectos da rede anônima que a tornam uma região única no ciberespaço.

Na terceira e última parte, nós buscamos fundamentar as razões que nos levam a crer que a rede TOR é um importante canal de comunicação, e relevante componente da estrutura do conhecimento no século XXI.

A princípio, a Internet era utilizada por uma elite técnica composta por cientistas da computação e entusiastas da área. Neste período, momento anterior a criação da "WWW" por Tim Berners-Lee, não havia as "janelas" de navegação que existem hoje; para usar a Internet, era necessário conhecer um mínimo de linguagem computacional. Para criar uma interface mais amigável da Internet, e resolver problemas de acesso à informação, Tim Berners-Lee criou o protocolo HTTP, responsável por fundar a World Wide Web (WWW), um sistema de conexão de páginas e servidores utilizando hyperlinks. Neste ambiente, surgem os motores de busca, como o Google, que navegam na WWW e armazenam cópias de páginas e conteúdos, além de endereços, em servidores próprios. No site de busca, estes motores são capazes de mostrar listas de resultados mediante a inserção de termos na barra de busca. Tudo o que não é catalogado por estes grandes motores de busca permanece "escondido" na vasta WWW, pois não são

mostrados por estes grandes “portais” de informações. A este conteúdo escondido dá-se o nome de Deep Web. É nesta região que classifica-se a Dark Web, e cuja rede TOR faz parte. Utilizando-se um software específico é possível o acesso a esta rede. Os atores não-estatais cuja atuação é estudada no último capítulo desta dissertação utilizam o TOR para dar cabo às suas atividades.

Em outras palavras, a compreensão do funcionamento técnico da Internet, para contextualizar e explicar a Dark Web e, especificamente, a rede anônima TOR, nesta pesquisa é fundamental para entendermos de que maneira, e em que medida, ocorre a difusão de poder nesta região do ciberespaço.

3.1 HISTÓRICO E FUNCIONAMENTO DA INTERNET ATÉ WORLD WIDE WEB

Quando se discute sobre a identidade do "pai da Internet", muitos autores e jornalistas creditam este título ao inglês Tim Berners-Lee, criador da World Wide Web – um sistema de navegação composto por páginas e hyperlinks nascidos em 1990. No entanto, o papel de Berners-Lee foi criar o sistema de navegação em interfaces amigáveis ao usuário, por meio de textos e janelas onde se poderia "saltar" entre as diferentes páginas com conteúdo. Ou seja, A Internet já existia quando ele criou a Web – o que esta última fez, foi permitir maior alcance da rede mundial de computadores por abrangir novos usuários que desconhecem a linguagem computacional. (CASTELLS, 2001). Para Naughton (1999), o título de "pai da Internet" é bastante disputado. Mas, segundo ele, Paul Baran tem as reivindicações mais sólidas. Ex-funcionário da Rand Corporation, Paul Baran foi responsável por desenvolver os princípios básicos por trás do sistema de redes na origem da Internet: os sinais digitais e os pacotes de dados.[74] Naquela época, o lançamento do satélite soviético Sputnik alimentou a corrida científica e tecnológica entre EUA e URSS. (NAUGHTON, 1999). Diante deste cenário, as Forças Armadas norte-americanas investiram em pesquisas que pudessem desenvolver tecnologias capazes de proteger as comunicações militares frente a possíveis ataques nucleares.

Em 1964, Paul Baran publica sua pesquisa acerca de um sistema de comunicação baseado em rede distributiva capaz de sobreviver a ataques físicos.[75] A sobrevivência das comunicações dependia, grosso

74 De acordo com Naughton (1999), a Rand Corporation era um "think tank" fundado, principalmente, pelas Forças Aérea dos EUA e que, em troca de investimentos, recebia relativa liberdade para realizar pesquisas. Muitas destas grandes pesquisas eram, geralmente, relacionadas com a área de interesse da Força Aérea. Quando Paul Baran chegou à Rand Corporation, em 1959, no auge da Guerra Fria, foi encarregado de investigar a possibilidade de preservação dos sistemas responsáveis por armas estratégicas de comando e controle no caso de ataques físicos. Existem outros nomes relevantes na trajetória de criação da Internet, além de Paul Baran. Banks (2008) lembra o papel de Leonard Kleinrock, cuja pesquisa de doutorado, sobre distribuição de dados em uma rede, resultou em livro publicado em 1964. Ceruzzi e Aspray (2008), por seu turno, atribuem a Donald Davies, físico britânico, o desenvolvimento e cunhagem do termo "*packet switching*" ("comutação de pacotes"), essencial para a construção de uma rede distribuída.

75 Estes primeiros sistemas de comunicação resistentes a ataques físicos foram, imaginados por Baran, de modo que pudessem resistir sem dependência de energia elétrica convencional : "Since destruction of the national electricity grid was an assumed

modo, da maneira em que os nódulos (o modo pelo qual ele designou as estações de comunicação) estavam conectados: (a) centralizados, perspectiva de sobrevivência rara; (b) descentralizados, perspectiva de sobrevivência baixa; (c) dispostos em rede distributiva, alta perspectiva de sobrevivência.[76] (BARAN, 1964).

O passo seguinte seria utilizar sinais digitais para percorrer a rede, uma vez que os sinais analógicos perdem sua qualidade à medida que percorrem as estações.[77] Segundo Baran (1964), as informações seriam transmitidas entre os nódulos utilizando blocos de mensagens padronizados. Estes blocos eram de tamanhos iguais e formados por segmentos de dados. Para viajar a rede até o destino final, os blocos de dados eram "desmontados" de modo que os seus segmentos percorreriam diferentes rotas. No destino, estes segmentos seriam ordenados novamente para dar lugar ao bloco de mensagem original, que seria lido pelo receptor. Os nódulos têm grande importância pois eles seriam responsáveis por escolher a melhor rota para o próximo segmento do bloco de mensagem, de modo que todos chegassem ao mesmo destino escolhido.[78] A razão para que chegassem todos ao mesmo destinatário se deve ao próprio bloco de mensagem: nele estão contidas informações que indicam o início da mensagem, endereçamento, emissor, precedência, "hand-over number", o próprio conteúdo da mensagem em formato de texto, e o final da mensagem (BARAN, 1964).

Uma metáfora interessante que auxilia a compreensão anterior desse processo é imaginar que a mensagem, emitida pelo emissor,

---

consequence of a nuclear exchange, the transmitter/receivers 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 Verificar "Anexo 3 – Redes Distributivas".

77 Os sinais digitais não degradam da mesma forma que os analógicos pois são apenas sequências dos algarismos "zero" e "um" – além de existirem técnicas suficientemente simples para checar se uma determinada sequência foi transmitida corretamente (NAUGHTON, 1999).

78 Naughton (1999, p.103) explica que, para que os nódulos pudessem escolher a melhor trajetória para cada segmento (menos custo, mais velocidade), Baran criou um algoritmo contendo uma tabela. Nesta tabela estavam informações sobre quantos "saltos" restavam para que o segmento chegasse ao próximo nódulo (nódulo vizinho). A tabela, assim, indicaria as melhores rotas, a qualquer momento, pois era regularmente alimentada por informações acerca do estado dos nódulos vizinhos – de modo que, se um nódulo pulasse fora dessa malha, a tabela era atualizada para refletir a mudança e, assim, os blocos de mensagem eram alterados para outras rotas.

completa é como se fosse um quadro de quebra-cabeças. Enviar o quadro inteiro pela rede (a informação) se mostrava uma tarefa desafiadora para os propósitos daquela época (manter os canais de comunicação intactos em caso de ataque físico à infraestrutura). É mais fácil desmembrar o quadro de modo que, ao final, existam apenas as peças do quebra-cabeça (segmentos de dados). Assim, elas são enviadas, individualmente, através da rede em direção ao receptor determinado. As diferentes peças seguem as mais variadas rotas, em diferentes velocidades, "lendo" constantemente a tabela com informações sobre a melhor rota (menor custo, mais velocidade). Quando chegam ao destino, estão "embaralhadas", mas atrás de cada pecinha existem instruções de sua posição para compor a imagem. As peças do quebra-cabeça são "lidas" e, desse modo, é possível recriar o quadro completo, tal qual na sua origem. O receptor final pode, então, observar o quadro em seu formato original na mensagem lida.[79]

Em suma, dois pontos são centrais no trabalho de Baran: que o número necessário de conexões para que cada cada estação de trabalho (nódulo) pudesse assegurar a sobrevivência de toda a rede era três (esta característica, número de conexões que garantem a sobrevivência, ele chamou de "redundância"); a segmentação dos blocos de mensagens em dados menores, capazes de serem transmitidos ao longo da rede até o destino final por meio de sinais digitais e rotas variadas (esta característica ele denominou "comutação de pacotes").

O trabalho original de Baran sobre a comutação de pacotes de mensagens ao longo de uma rede distribuída originou os fundamentos por trás da comunicação em rede que possibilitou o surgimento da Internet – a rede feita de redes cujo alcance na década de1990 se tornou global.

3.1.2 Protocolo TCP/IP

79 Este sistema é um pouco diferente na rede anônima TOR: também existem blocos de mensagens e segmentos de dados, porém, as informações atrás de cada "pecinha de quebra-cabeça" está escondida debaixo de camadas de criptografia – e cada camada apenas pode ser "lida" por um único nódulo. Não há como ler todas as camadas de uma única vez. Outra diferença é em relação ao endereçamento. Cada nódulo apenas saberia o endereço do próximo nódulo a enviar a peça, mas não o nódulo final. Estas e outras características compõem a tecnologia da rede TOR que a diverge da rede Internet – e, assim, tenta proteger mensagens e usuários. Mais sobre isso em seções posteriores.

A origem da Internet como a conhecemos é a ARPANET – uma rede desenvolvida entre cientistas e entusiastas da computação abrangendo cinco universidades norte-americanas cujos estudos foram financiados pelos militares-norte americanos. O nome da rede deriva do nome DARPA (Defense Advanced Research Projects Agency). Para que os computadores digitais possam comunicar-se entre si através da rede eles precisam adotar o mesmo conjunto de regras – ou protocolos.[80] Caso contrário, cada máquina apenas entenderia ela mesma. O protocolo fundamental adotada pela rede ARPANET para a transferência de dados foi o TCP/IP. (CANABARRO, 2014).

Duas observações sobre os protocolos são pertinentes. Primeiro, os atos de segmentar os dados em pacotes e remontar os pacotes de dados (para que se transformem na mensagem original) precisam ser gerenciados por um conjunto de regras adotado pelo computador emissor e pelo computador receptor. Ou seja, os computadores precisam obedecer as mesmas regras de segmentação e reconstrução de pacotes. Segundo, os computadores precisam saber sua posição e a posição dos demais computadores na rede. Cada computador é um nódulo, e o conjunto de nódulos forma a "rede". Portanto, sabendo a posição dos dispositivos na rede permite que os computadores saibam o destino de cada pacote e se ainda existe rota a percorrer ou não. A partir da ARPANET, o protocolo TCP/IP popularizou-se e, assim, tornou-se o mais utilizado para a transferência de dados em rede. (LAKSHMAN; MADHOW, 1997). Seu nome advém da junção de dois protocolos específicos: *Transmission Control Protocol* (TCP) e o *Internet Protocol* (IP). Este protocolo garante o envio, o deslocamento e a chegada dos pacotes por meio de um conjunto de regras específicas em cada momento da transferência de dados. Este conjunto de regras são adotadas por todos os computadores da rede. As regras atuam em cima (a) da segmentação do bloco de mensagem em parcelas menores – estes são os pacotes de dados que navegam pela rede; (b) do procedimento de endereçamento de cada parcela (partida e chegada); (c) o deslocamento dos pacotes através das melhores rotas (menos custo, mais velocidade) na rede até o destino final; (d) montagem ordenada e integral dos

80 De acordo com Ceruzzi e 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."

pacotes, no destino final, de modo a se obter o bloco de mensagem original. (CANABARRO, 2014).

Nauhton (1999) explica o funcionamento do TCP-IP de modo similar ao exemplo do quadro de quebra-cabeças, onde a imagem geral é dividida em menores (pecinhas do quebra cabeça) que viajam pela rede individualmente e sendo remontadas apenas no destino final para surgir a imagem geral do início. Ele relata a experiência de realizar uma busca, no motor de busca AltaVista ("portais" de informações da web), bastante popular na década de 1990, analisando os procedimentos do seu computador e da rede no envio e recebimento dos pacotes de dados. Ele diz

> 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 "packetswitched" 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).

Mas o protocolo TCP/IP não é o único protocolo utilizado na rede. Dois dos primeiros protocolos foram o *TELNET Protocol* e o *File Transfer Protocol* (FTP) – protocolos assimétricos (unilateral) que permitiam a troca de arquivos de um computador servidor para um computador cliente. Na sequência, surgiu o *Network Control Protocol* (NCP), o primeiro software de comunicação interprocessada da ARPANET e um protocolo simétrico, ou seja permite o estabelecimento da comunicação entre dispositivos a partir do computador servidor ou computador cliente.[81] Surgiu também o *Message Transmission Protocol*

81 O protocolo NCP foi substituído, posteriormente, pelo protocolo TCP/IP (NAUGHTON, 1999).

(MTP), que tratava das mensagens eletrônicas (*eletronic mails* ou e-mails) (NAUGHTON, 1999). Durante este período inicial de desenvolvimento da rede (que viria ser mundial), os cientistas e entusiastas da computação trabalhavam de modo aberto e colaborativo na criação de protocolos que pudessem ser adotados por todas as máquinas da rede assim elas utilizariam a mesma "linguagem" para trocar informações específicas. Esta característica, de trabalho aberto e colaborativo, é apontada por Castells e Cardoso (2005) como essencial para que a Internet se tornasse aberta e plural. Além dos já mencionados, outros protocolos ainda utilizados na atualidade são: *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), e outros.

Quando Tim Berners-Lee criou o sistema de navegação da rede, em 1990, com endereços, páginas, hyperlinks, utilizando um navegador, a Internet já era real. Diversos computadores digitais localizados em diferentes regiões geográficas transmitiam dados e informações entre si. Entusiastas e acadêmicos trocavam arquivos e imagens, mantinham conexões por voz, enviavam e recebiam mensagens instantâneas (os "Chats") e e-mails, entre outras coisas. A World Wide Web, portanto, se assentou sobre bases já consolidadas, operando sobre uma Internet existente. Sua principal característica talvez tenha sido tornar sensorial a experiência de uso da Internet, possibilitando que o usuário "navegasse" entre janelas e conteúdos com o clique do mouse.

3.1.3 A World Wide Web (WWW)

O britânico Tim Berners-Lee trabalhava no CERN[82] ao final da década de 1980 e desenvolveu a web nos meses entre março de 1989 e

82 A sigla CERN deriva do acrônimo francês Conseil Europeen pour la Recherche Nucléaire, e é uma organização mais conhecida por sua alcunha na língua inglesa, European Organization for Nuclear Research (CERN). O CERN é a organização européia para pesquisas nucleares, fundada em 1954 na fronteira franco-suíça. Inicialmente, preocupava-se com estudos relacionados ao átomo mas, atualmente, dedica-se a pesquisas relacionadas, principalmente, às partículas físicas. (EUROPEAN COUNCIL FOR NUCLEAR RESEARCH, 2017).

novembro de 1990. Inicialmente, Berners-Lee identificou um problema no ambiente de trabalho: o centro de pesquisas tinha grandes dificuldades de armazenamento e transmissão de informações e documentos entre os cientistas. Para "piorar" este quadro, os cientistas trabalhavam em sistemas de alta rotatividade, visto que muitos ali estavam por período de tempo delimitado. Este problema dificultava, em grande medida, a eficiência das pesquisas e do CERN em geral. A solução, encontrada por Berners-Lee, foi criar um sistema de informação interconectada. Para construir este sistema, ele se serviu da jovem Internet, uma rede de transmissão de dados de longas distâncias que utiliza computadores digitais. (NAUTHTON, 1999)

Em novembro de 1990, em uma tentativa de operacionalizar tal solução, Berners-Lee iniciou atividades de programação e desenvolveu um software – o qual chamou de "*browser*", ou "navegador". Este software, na prática, criava uma "janela" virtual na interface do computador que mostrava a estrutura do ciberespaço (Ibid., 1999).

Mas apenas o navegador não era suficiente. Naughton (1999) argumenta que o criador da Web precisou assegurar que as informações públicas, armazenadas em outros computadores na rede, pudessem ser acessadas através do navegador que criara. Para isto, ele começou a desenvolver um conjunto de protocolos que atuavam sobre o navegador que ele já criara. Assim, se todos os computadores adotassem as mesmas linguagens sobre o sistema de "janelas" (navegadores) que ele havia criado, estes diferentes computadores digitais que habitavam a rede mundial poderiam comunicar entre si *através do próprio navegador*. Ou seja, a comunicação entre eles poderia acontecer apenas através das "janelas".

Em especial, dois protocolos e uma linguagem própria foram essenciais para o funcionamento da Web além do software navegador: (1) um primeiro protocolo para especificar a localização do armazenamento da informação dentro dos computadores (este protocolo era análogo ao protocolo IP – que especifica a localização de cada máquina conectada na rede mundial de computadores), ao qual Berners-Lee chamou de "*Uniform Resource Locator*" (URL); (2) um segundo protocolo para especificar de que modo a informação deveria ser trocada entre as máquinas (este protocolo também era análogo ao protocolo FTP – que especifica o modo como os arquivos são transmitidos na rede mundial de computadores), a qual ele chamou de "*Hyper Text Transport Protocol*" (HTTP); (3) e uma linguagem de computação própria que ele denominou de *Hyper Text Mark-up Language* (HTML), que se tornou o

"idioma" de toda a Web criada por ele. Entre a concepção da ideia e a criação do navegador (e protocolos inerentes) o criador da Web levou pouco mais de um ano (Ibid., p.239-240).

A Web desenvolvida por Berners-Lee se tornou pública em janeiro de 1991. Nesta época, ela era apenas uma entre as diversas outras aplicações que percorriam a rede – que, no entanto, ainda não havia ganhado popularidade.[83] (Ibid.). Cabe lembrar que a Internet já existia e era utilizada no momento da criação do britânico. Apesar de não existir navegadores, ou "janelas" de interfaces amigáveis, os usuários que já operavam na Internet eram capazes de transmitir informações e dados entre os computadores – bastava conhecimento técnico e linguagem de programação para tanto. Este fato, lembra Ceruzzi (2008), é um dos pontos que manteve a Internet, até aquele momento, como um meio de comunicação elitista – muito embora fosse calcado na cultura da liberdade e no sentimento de comunidade que envolvia os acadêmicos e entusiastas da computação, especialmente na sua origem. Foi Marc Andreessen que potencializou o sistema de navegação criado por Tim Berners-Lee e trouxe um mundo de cores, imagens e vídeos para a "janela" interativa e permitiu que a Internet se tornasse popular.

Em janeiro de 1993, Marc Andreessen tornou público o navegador Mosaic. Ele foi seu co-criador, juntamente com Eric Bina (CERUZZI, 2003). Este novo software, além de gratuito, trazia outras novidades: era possível anexar imagens aos textos na janela de navegação e podia ser instalado em computadores simples – ao contrário das estações de trabalho UNIX, muito populares (NAUGHTON, 1999). Andreessen tinha como objetivo acabar com os obstáculos remanescentes que separavam a elite dos entusiastas da computação e o público geral. E conseguiu pois, a partir do Mosaic, a "aplicação" Web ocupou a maior parte da rede mundial de computadores. Os criadores do navegador Mosaic também foram responsáveis por desenvolver o Netscape Navigator, uma versão progressista do Mosaic: visualmente mais "limpo", seguro, com apoio para layouts elegantes e documentos

83 Naughton (1999, p.248) traz uma tabela em que mostra, proporcionalmente, o tráfego de protocolos utilizados no backbone da Internet da National Science Foundation (NSF) – ou seja, principal backbone da Internet à época. Em 1993, o protocolo FTP era o mais utilizado, compondo 42,9% do tráfego de dados. Enquanto isso, o protocolo da Web era responsável por 0,5% do tráfego de dados. Dois anos depois, em 1995, o protocolo FTP compreendia 24,2% do tráfego de dados, enquanto o protocolo da Web respondia por cerca de 23,9% – tornando-se o protocolo mais utilizado na rede mundial de computadores. Ver ANEXO 4 – Tráfego de Dados por Protocolo no "NFS Internet Backbone".

elaborados, além de ser muito mais rápido (Ibid., 1999). O Netscape Navigator foi comercializado e abriu capital na bolsa de valores em 8 agosto de 1995. Ao final deste dia cada ação custava 58 dólares norte-americanos; poucos meses depois, cada ação custava 150 dólares norte-americanos (CERUZZI, 2003).

A criação da WWW por Tim Berners-Lee, os navegadores Mosaic e Netscape Navigator criados por Marc Andreessen, a ampla adoção dos protocolos TCP/IP e DNS são os desenvolvimentos técnicos que permitem que a Internet seja expandida e ganhe contornos mundiais, uma vez que seu uso torna-se simples para a parcela dos indivíduos que não lidam com computação diretamente. (CANABARRO, 2014). Outro aspecto, embora não técnico, que contribuiu para isso foi a comercialização da Internet: "A partir da comercialização do serviço de acesso à Rede como desenvolvimento político-econômico da Era Digital, o uso da Internet passou a abarcar as mais variadas áreas da atividade da vida humana e, com isso, a ter implicações socioeconômicas, políticas e culturais […]." (CANABARRO, 2014, p.94).

Naturalmente, com a Internet visualmente amigável, disponível à navegação pelo público em geral (e não mais apenas os entusiastas), aberta à comercialização, acessível por meio de navegadores que trouxeram textos, figuras e dinâmica para a rede, o próximo passo foi o desenvolvimento dos grandes motores de busca como o AltaVista, Yahoo!, Google. Estes "motores" eram responsáveis por realizar pesquisas na vasta quantidade de informações disponíveis na Web. Ou seja, eram "facilitadores" da navegação: ao invés de o usuário buscar individualmente cada página atrás de conteúdo de seu interesse, estes motores traziam uma listagem de páginas como resultado de uma busca por termo definido por ele. Caso o usuário desejasse encontrar páginas na Web cujo conteúdo se relacionasse ao cinema norte-americano, por exemplo, bastava que ele inserisse termos relacionados ao cinema norte-americano na barra de busca destes motores. Na sequência, eles listariam os resultados dessa busca no formato de um grande índice de páginas – acessíveis por hyperlinks. Tudo que era listado como resultado ficou, posteriormente, conhecido como Surface Web. Tudo o que permanecia alheio, e portanto não aparecia em nenhuma listagem de resultado de nenhum motor de busca, ficou conhecido, na literatura do assunto, como Deep Web. Estes serão os temas abordados na próxima subseção.

3.1 SURFACE WEB E DEEP WEB: DIVISÃO DAS ÁGUAS DIGITAIS

Em setembro de 2001, Michael K. Bergman, pesquisador do Bright Planet, publicou um artigo intitulado *The Deep Web: Surfacing Hidden Value* tratando, especificamente, da Deep Web.[84] No artigo, Bergman (2001) cita que realizou a pesquisa baseada na coleta de dados, realizada entre 13 e 30 de março de 2000 e admite que sua pesquisa é o primeiro estudo de quantificação e caracterização da Deep Web. De acordo com ele, a Deep Web se refere ao conteúdo informacional disponível pela Web que não é indexado, ou possível de ser buscado, pelos motores de busca convencionais.[85]

Destacamos quatro pontos da pesquisa conduzida por Bergman (2001): (1) o estudo buscou quantificar o tamanho da Deep Web e concluiu que ela é cerca de 400 a 550 vezes maior que a Surface Web; (2) características gerais da Deep Web envolvem o tamanho de suas páginas, muito maiores que as páginas da Surface Web, e o tamanho dos seus documentos, cerca de 27% menores que os documentos da Surface Web – além de indicar que cerca de 97,4% da Deep Web é composta de páginas públicas acessíveis sem restrição; (3) os motores de busca adotam critérios para a indexação de páginas nos seus bancos de dados – e, consequentemente, critérios para não indexar muitas páginas da Web; (4) os dados são antigos, do ano 2000, mas, devido a escassez de estudos quantitativos sobre este objeto, ainda permanecem relevantes como ponto de partida. [86]

---

84 Este artigo tornou-se referência nos estudos sobre o assunto Deep Web, listado como o artigo mais citado pelo banco de dados "SCOPUS" em 2017, utilizando o termo (entre aspas) "Deep Web".

85 O pesquisador opta pela utilização do termo "Deep Web" ao contrário do termo "Invisible Web", cunhado por Jills Ellsworth em 1994, para designar o conteúdo informacional "invisível" aos motores de busca convencionais. Segundo Bergman (2001), esse conteúdo é "visível" e possível de ser acessado por métodos não-convencionais. Por este motivo, ele abandona o termo e passa a adotar "Deep Web". No entanto, Sherman e Price (2001) utilizam o termo original "Invisible Web" para tratar do mesmo objeto (utilizando também o termo "dark matter", que não deve ser confundido com o termo "Dark Web" ou "Darknet"), além de categorizar a "Invisible Web" em quatro regiões.

86 Bergman (2001, p.1) indica que a Deep Web contém cerca de 7.500 terabytes de informação comparados com 19 terabytes de informação da Surface Web. Em termos de documentos individuais, a Deep Web contém, aproximadamente, 550 bilhões de documentos – enquanto a Surface Web compreende cerca de 1 bilhão de documentos individuais. Os estudos de Sherman e Price (2001, p.82) indicam outros dados: excluindo-se ferramentas especiais de busca e dados irrelevantes para pesquisadores (ou usuários

No Brasil, Fidêncio e Monteiro (2013) apontam a literatura de Bergman (2001), Sherman e Price (2001) como as bases sobre as quais os demais estudos acerca do assunto se desenvolveram. De acordo com eles, Bergman (2001) foi responsável por trazer a dimensão quantitativa sobre a Deep Web, enquanto Sherman e Price (2001) buscaram categorizá-la. Estes últimos deram origem a quatro classificações de "invisibilidade"[87]: Opaque Web; Private Web; Proprietary Web e Invisible Web[88]. Segundo os autores, "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). A categoria "Dark Web" foi descrita por Becket (2009).

Na sequência, descrição das quatro distintas Webs descritas por Sherman e Price (2001) e, posteriormente, descrição da "Dark Web" como definida por Becket (2009).

3.2.1 Opaque Web

De acordo com Sherman e Price (2001), a Opaque Web ("Web Opaca") é composta por aquivos que não foram incluídos nos índices dos motores de busca *apesar* de, tecnicamente, serem capazes. Ou seja, não há nenhum obstáculo técnico que impeça que este conteúdo seja indexado.

Existem razões para que este conteúdo informacional não seja indexado pelos motores de busca e os pesquisadores elencam quatro: (1) profundidade de alcance dos "robôs" [89], já que existe um custo

---

que executam buscas), estima-se que a "Invisible Web" seja entre 2 a 50 vezes maior que a "Visible Web". Contudo, outras pesquisas quantitativas acerca do assunto também foram elaboradas por He et al (2007).

87 Cabe lembrar que Sherman e Price (2001) utilizam o termo "Invisible Web" para tratar do que Bergman (2001) chama de "Deep Web" – razão para denominarem as quatro categorias definidas por eles de acordo com graus de "visibilidade". O termo "Deep Web" se popularizou.

88 Fidêncio e Monteiro (2013) elaboraram figura esquemática baseada na literatura de Sherman e Price (2001), adaptada do esquema semelhante ao de Ford e Mansuriam (2006). Ver "ANEXO 5 – As várias Webs".

89 De acordo com os autores, os motores de busca lançam "robôs" (sofwares) que realizam uma "varredura" na teia da Web, acessando páginas e mais páginas (pulando entre elas através dos hyperlinks) e copiando e listando estas páginas em grandes banco de dados. Estes robôs também são conhecidos por "aranhas" ("spiders", já que sua função é caminhar pela "teia", ou "web"). Outro nome utilizado é o de "crawlers" (ou "rastejadores"). (SHERMAN; PRICE, 2001, p.15). Acredito que "varredores" também

envolvido na "varredura" da Web pelo motor de busca; (2) frequência da varredura – a web possui um caráter dinâmico, com inúmeras páginas sendo adicionadas diariamente, o que significa que cada motor de busca deve tomar decisões sobre a frequência das varreduras realizadas pelos "robôs" que realizam a indexação das páginas. Os "robôs" precisam se certificar que a página ainda é válida, ou atualizá-la no seu índice; (3) número máximo de resultados visíveis – cada motor de busca determina a quantidade máxima de resultados listados para o usuário em cada busca; (4) URL's desconectadas – páginas que não são submetidas diretamente aos motores de busca, e que não possuem links externos em outras páginas apontando para si, são chamadas de "URL's desconectadas" e não podem ser indexadas porque o robô não tem como achá-las.

De modo resumido, Sherman e Price (2001) concluem afirmando que " […] 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

A Private Web ("Web Privada") consiste de páginas da Web que são tecnicamente possíveis de indexar pelos motores de busca mas que foram excluídas deles por razões deliberadas. A Private Web, de modo geral, compõe-se de regiões da Web cujo acesso não é público – apenas aos usuários com permissões para acessar as páginas. (Ibid., p.73). Além disso, existem três modos de excluir uma página do alcance dos motores de busca: (1) implementar o uso de senha para acessar o conteúdo da página, já que os robôs que realizam as varreduras na web não conseguem ultrapassar este obstáculo; (2) utilizar o arquivo de texto "robots.txt"[90] para informar ao robô varredor da não indexação da

seja um termo adequado visto que os "robôs" realizam uma varredura da Web em busca de conteúdo informacional passível de indexação.

90 Sherman e Price (2001) discutem sobre os robôs e buscam define-los do seguinte modo: "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

página; (3) utilizar a meta tag "no index"[91] para prevenir o robô varredor de ler além do conteúdo de cabeçalho da página e, assim, indexar o corpo da página.

Os pesquisadores enfatizam ainda que o primeiro método, a implementação de senha para o acesso, é uma técnica mais forte em comparação com as outras duas porque faz uso de uma barreira especificamente técnica ao contrário de um padrão voluntário.

3.2.3 Proprietary Web

A "Proprietary Web" é composta por páginas cujo acesso só é permitido por meio de acordos de termos especiais. Ou seja, os motores de busca não podem indexá-las porque seu acesso depende destes termos (aceitos em troca da visualização do conteúdo). Entram nesta categoria conteúdo acessível por meio de registros gratuitos; registros pagos mediante uma taxa; registro de inscrição para acesso a conteúdo; inscrição em "newsletters"; etc. Os "robôs" varredores não conseguem satisfazer as requisições mais simples de registro e, por esta razão, não são capazes de indexar o conteúdo das páginas posteriores à tela de inscrição/registro. (SHERMAN; PRICE, 2001, p.296). Os autores ainda oferecem alguns exemplos de páginas que pertencem à categoria "Proprietary Web".

3.2.4 Truly Invisible Web

Os autores chamam a "Invisible Web" também de "Truly Invisible Web". Isto é feito para não confundir o leitor entre os termos "Invisible Web" (dentro da qual estão as categorias "Opaque Web", "Private Web", "Proprietary Web" e "Truly Invisible Web").

---

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 Especificamente sobre isso, eles argumentam que "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)

Eles ressaltam o cuidado com a definição da categoria "Truly Invisible Web" pois tal definição deve ser fluida de modo a cobrir novos formatos de documentos e páginas – uma vez que os robôs varredores dos motores de busca estão em constante adaptação e progressão em termos tecnológicos. Neste sentido, os pesquisadores destacam três principais fontes de conteúdos informacionais que pertencem à categoria "Truly Invisible Web": (1) páginas da Web cujo formato ainda não são geridos pela categoria atual de robôs varredores, que segundo eles envolvem documentos no formato "PDF", "Shockwave", "PostScript", "Flash", etc.[92]; (2) páginas da Web geradas dinamicamente, especificamente a partir de requisição que utiliza um "script" não-interativo para gerar a página[93]; (3) conteúdo informacional alocado em bases de dados relacionais[94], pois não há como extrair a informação sem realizar uma inquisição ao banco de dados.

3.2.5 Dark Web

A "Dark Web", muitas vezes entendida como "Darknet", não faz parte das categorias iniciais definidas por Sherman e Price (2001). Fidêncio e Monteiro (2013) apontam que esta nova "parte" da Web surge posteriormente na literatura com Andy Becket, em artigo publicado pelo jornal "The Guardian", na seção de Tecnologia, no ano de 2009.[95]

92 Na época da escrita do livro, em 2001.

93 O problema, de acordo com os autores, é o uso indiscriminado de "scripts" que levam aos robôs varredores em "armadilhas de aranhas" em que eles ficam, literalmente, presos dentro de um conjunto de milhares, ou milhões, de páginas unicamente para afugentar os motores de busca. (SHERMAN; PRICE, 2001, p.74-75). Segundo a definição da 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 Duas observações em relação ao termo "Dark Web". Este termo também foi utilizado por Hsinchun Chen, professor da Universidade do Arizona, diretor e fundador do Laboratório de Inteligência Artificial (AI LAB), em 2006, na obra "Intelligence and Security Informatics for International Security". O sentido dado pelo professor Chen é diferente. Ele utiliza o termo "Dark Web" para denominar pesquisas, na área da informática, relativas ao fenômeno do terrorismo – em especial no âmbito do projeto "Dark Web Portal". Outro sentido ao termo "Dark Web" foi proferido pelo co-fundandor do software

De modo específico, a Dark Web compreende os conteúdos que foram intencionalmente ocultados de terceiras pessoas. (FINKLEA, 2015). Outra definição semelhante, levantada por Becket (2009) é que a Darknet é uma rede online escondida para não-usuários. Já Biddle et al (2002) afirmam que a Darknet é "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) Para fins de definição desta pesquisa, designa-se Dark Web ao conjunto de redes online anônimas que realizam um esforço ativo para manterem-se ocultas de não-usuários, utilizando, para isto, uma camada de aplicação e protocolo criados sobre redes físicas existentes. Por esta razão, a Dark Web é composta de redes anônimas – como as redes Freenet, The Onion Router (TOR) e The Invisible Internet Project, (I2P).[96].

Apesar de não fazer parte das categorias inicialmente descritas por Sherman e Price (2001), Fidêncio e Monteiro (2013) realizam tentativa de contextualizá-la nas escrituras daqueles: "[...] é bastante seguro considerar a Dark Web como uma nova ramificação da Web Invisível [segundo definido por Sheman e Price (2001)]: suas características são próprias; sua filosofia é própria e, além de tudo, seu conteúdo é o mais enigmático e desordenado de todas as ramificações". (FIDÊNCIO; MONTEIRO, 2013, p.692). E complementam, afirmando ainda que "Na Dark Web o anonimato é desejável aos utilizadores, principalmente por causa de posições filosóficas dos usuários ou alguma posição contrária às normas sociais." (Ibid., p.693).

TOR, Roger Dingledine, durante a convenção "DEF CON Hacking", em julho de 2017. Na ocasião, Dingledine realizava críticas aos jornalistas que apresentavam o software TOR como um espaço dominado por serviços ilícitos (que, segundo ele, apenas representa as atividades de 3% dos usuários da rede TOR). A estes serviços ilícitos, nesta ocasião, Dingledine chamou de "Dark Web" – afirmando que esta "Dark Web" não existia [proporcialmente]. (THOMSON, 2017) A pesquisadora Mary McEvoy Manjikian também utilizou o termo neste sentido, afirmando "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). Por último, o termo "Darknet" é utilizado pelo projeto Freenet para indicar a rede anônima instalada entre nódulos de amigos, ao contrário de "Opennet" que é uma rede anônima instalada entre nódulos de desconhecidos. (FREENET, 2017). Nesta pesquisa, utilizaremos o termo no sentido conferido por Finklea (2015).

96 A origem da Dark Web refere-se a criação da primeira rede anônima – neste caso, a rede Freenet. Baseada no trabalho de conclusão de curso, em Ciência da Computação e Inteligência Artificial, de Ian Clarke: "A Distributed Decentralised Information Storage and Retrieval System", de 1999, pela Universidade de Edinburgh. A rede Freenet, acessada mediante software de mesmo nome, foi lançada no ano seguinte.

A definição de "Dark Web" utilizada nesta pesquisa encontra origem em artigo de Andy Becket, 2009, que afirma que "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). Nesta linha, Chertoff e Simon (2015), da Chatam House, The Royal Institute of International Affairs, adotam o sentido de "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) Essas ideias são complementadas por trabalhos posteriores como o de Devine, Egger-Sider e Rojas (2015). Eles também afirmam que a Dark Web é uma porção menor da Deep Web e que foi intencionalmente escondida e, por esta razão, torna-se inacessível através de navegadores web convencionais.

Finklea (2015) utiliza o conceito também no sentido da Dark Web ser uma das regiões da Deep Web que contém conteúdo que foi intencionalmente escondido e cujos usuários podem acessar através do uso de softwares especiais como o TOR. Além disso, afirma que esta região pode ser acessada para propósitos legítimos e para esconder atividades maliciosas ou criminosas, sendo que foi a exploração da Dark Web para práticas ilegais que ganhou o interesse das autoridades e decisores políticos. Roche (2016) identifica a Dark Web como sendo um mundo escondido atrás da criptografia, tecnologias peer-to-peer e de anonimato que mascaram os endereços de IP para ocultar a localização do usuário.

Para acessar a Dark Web, é necessário o uso de algumas "ferramentas" – usadas por ativistas de direitos humanos para criar um sistema de comunicação online em redes de malhas wireless – como o software livre TOR, que oferece anonimato, a plataforma peer-to-peer I2P, o software Freenet e o Projeto Darknet. Os pesquisadores Zulkarnine et al (2016, p.109) salientam as características da Dark Web.

97 O sufixo ".onion" indica navegação em conteúdo proveniente da rede online TOR, acessado por software não-convencional de mesmo nome. Já o sufixo ".i2p" indica navegação em conteúdo proveniente da rede online I2P, também acessado por software não-convencional de mesmo nome.

São elas: a descentralização, o uso da infraestrutura da internet[98] e o uso de protocolos e portas não-convencionais que são inalcançáveis por aqueles de fora da rede. No direito, destaca-se o estudo de Ghappour (2017, p.1077) que define a Dark Web como sendo uma rede global de computadores que utilizam protocolos criptografados para comunicar, permitindo que os usuários conduzam transações de modo anônimo sem revelar suas localizações.

Sendo assim, levantamos quatro pontos importantes e comuns às definições identificadas nesta seção: (1) a Dark Web é parte da Deep Web; (2) ela corresponde a uma região da Web intencionalmente escondida; (3) para acessá-la é necessário o uso de softwares de navegação não-convencionais; (4) utiliza-se do anonimato para blindar as comunicações e a localização do usuário de terceiros.

Deste modo, a partir das definições trabalhadas, utilizamos o seguinte conceito de "Dark Web": região da Deep Web composta por redes online, ocultas para não-usuários e que utilizam o anonimato para blindar a comunicação e a localização do usuário, cujo acesso se dá por meio de softwares de navegação não-convencionais. (BECKET, 2009; CHERTOFF, SIMON, 2015; DEVINE, EGGER-SIDER, ROJAS, 2015; FINKLEA, 2015; GEHL, 2016; ROCHE, 2016; GHAPPOUR, 2017). Salientamos, contudo, a existência de outras definições, não adotadas por esta pesquisa, mas que também são discutidas na literatura do tema.[99]

---

98 De acordo com eles, a Dark Web é construída acima da Internet pública.

99 Biddle et al (2002) definem a "Darknet" como uma rede que emerge da ampla troca de objetos que podem ser copiados e distribuídos entre os usuários da rede conectados por canais de alta largura de banda. A ideia é capturar a noção de distribuição em massa de objetos entre milhares ou milhões de usuários. Já Everett (2009) elucida distinções entre os termos "Dark Internet", "Dark Web" e "Darknets". De acordo com ela, "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) sintetiza as definições de Everett (2009) e conclui que a "Dark Web is an amorphous collection of Internet sites that run on darknets,

Três redes fazem parte da Dark Web, definida acima: a pioneira "Freenet", que surgiu no ano 2000; a rede "TOR", que nasceu em 2002; e a rede "I2P", cuja origem foi no ano de 2003. Por fins de recorte de pesquisa, optamos por analisar, especificamente, a rede TOR. Para Moore e Rid (2016, p.9) o "Projeto TOR", responsável pelo gerenciamento da rede, é uma das plataformas de encriptação mais controversas e sofisticadas nos dias de hoje. Segundo os autores, "a arquitetura fluida destas redes [Freenet, I2P e TOR] torna a estimativa de tamanho difícil, mas parece que TOR é a maior [rede], com o I2P em um distante segundo lugar. Outros são significativamente menores em escopo e popularidade." (MOORE; RID, 2016, p.15, tradução nossa).

Na próxima seção, abordaremos com detalhe a rede TOR abrangendo os seguintes assuntos: o que é a rede; para que serve; seu histórico de desenvolvimento; funcionamento técnico; "serviços ocultos" (ou, de acordo com a literatura do assunto, "hidden services"); popularidade; aspecto político e características próprias. O objetivo é descrever sua importância política (que nos interessa) a partir do seu histórico, funcionamento e popularidade atual.

3.2 DARK WEB POR MEIO DA REDE TOR

A rede The Onion Router (TOR) é uma rede de "anonimização" de baixa latência para tráfego TCP.[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). Em outras palavras, é uma rede de comunicação anônima com milhares de nódulos roteadores ao redor do mundo.[101] (EDMAN; SYVERSON, 2009). O caráter anônimo deste sistema de comunicação

---

or overlay networks that employ non-standard communication protocols in order to encrypt and anonymize information." (PACE, 2016, p.2-3)

100 Que confere o anonimato.

101 A rede TOR utiliza a própria infraestrutura da rede mundial de computadores, atuando no tráfego de dados – responsabilidade do protocolo TCP – e baseia-se "on a client-server architecture model". (ALSABAH; BAUER; GOLDBERG, 2012, p.74). Na prática, isso significa que a rede utiliza os mesmos princípios básicos do protocolo para o tráfego de dados da própria Internet (por esta razão, dizemos que utiliza a mesma infraestrutura).

digital permite que seus usuários naveguem na Internet sem revelar suas identidades ou localizações. (LOESING, MURDOCH, DINGLEDINE, 2010;ELAHI et al, 2012). Na prática, configura-se como um popular sistema de aprimoramento da privacidade que é projetado para proteger a privacidade dos seus usuários contra os ataques de análise de tráfego lançados por um adversário não-global. [102] (MCCOY et al, 2008, p.63). Além disso, o TOR foi desenhado de modo a atuar nas aplicações de TCP – como a Web e as mensagens instantâneas, por exemplo. (LI et al, 2010). Por esta razão, seu uso é destinado à "navegação" da Web e, por isto, dizemos que é uma rede "de baixa latência".

A origem do TOR é derivada de um projeto colaborativo entre a organização sem fins-lucrativos "Free Haven Project"[103] e o Laboratório de Pesquisa Naval dos Estados Unidos da América ("US Naval Research Laboratory"), sob o Escritório de Pesquisa Naval dos Estados Unidos da América ("US Office of Naval Research"), financiado pela Agência de Projetos Avançados de Pesquisa de Defesa ("Defense Advanced Research Projects Agency", DARPA). (DINGLEDINE; MATHEWSON; SYVERSON, 2007). O objetivo deste projeto colaborativo era criar uma rede distributiva, anônima, criptografada e que fosse fácil de ser implementado de modo que pudesse ser utilizado por aqueles que necessitassem. A rede TOR foi oferecida como um serviço gratuito para promover o acesso sem restrições à Internet em locais onde ocorressem forte censura online, ou onde a ameaça de perseguição àqueles que buscassem acessoa a informações locais ilegais era real. (MOORE; RID, 2016). O software TOR foi desenvolvido em setembro de 2002. (AKHOONDI; YU; MADHYASTHA; 2012). Seu lançamento foi em 2003. (ELAHI et al, 2012; DINGLEDINE; MATTHEWSON; SYVERSON, 2007). Em 2005, dois anos após seu lançamento, a Eletronic Frontier Foundation (EFF), decidiu financiar os esforços da Free Haven Project por um ano,

102 Usar a Internet significa que os dados da sua máquina percorrem a rede mundial de computadores de modo eficiente. Por isto é possível a navegação. Na busca pela identidade de usuários da rede, agentes realizam ataques sobre o tráfego de dados. Dessa forma, o tráfego é analisado (comportamento, intensidade, rota, etc.) na tentativa de se estabelecer um padrão e, assim, facilitar a identificação de usuários. Edman e Syverson (2009, p.380) explicam isso com mais detalhes ao afirmar que "Tor aims to provide anonymity to clients by sending multiplyencrypted 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."

103 O "Free Haven Project" teve seu início em 1999, como um projeto de pesquisa composto por alunos do Massachussets Institute of Technology (MIT) com o objetivo original de criar um porto de dados gratuito e funcional. (FREE HAVEN, 2017).

com o objetivo de ajudar a manter as liberdades civis de cidadãos comuns no domínio cibernético. Desde 2006, o Tor Project se torna uma organização sem fins-lucrativos e passa a ser financiada por grupos comprometidos com o ativismo em torno do bloqueio online e a censura na Internet[104]. (DINGLEDINE; MATTHEWSON; SYVERSON, 2007). Em suma, a concepção do software se deu através de um projeto colaborativo entre sociedade civil, na figura da organização Free Haven Project, e Estado – por meio do Laboratório de Pesquisa Naval dos Estados Unidos, cujo financiamento foi providenciado pela DARPA . Cabe lembrar que a DARPA também participou da criação e do progresso da Internet nas décadas anteriores.

Na sequência, discutiremos o histórico do desenvolvimento do software TOR seguido de seu funcionamento; os serviços "ocultos" ("hidden services") que geram consequências "inesperadas" do uso da ferramenta; a popularidade do software TOR e seu caráter político no século XXI; características gerais; e, finalmente, a estrutura do conhecimento no século XXI e o *cyberpower* que se origina do ciberespaço. O objetivo é descrever os processos ideológicos e criativos que permitiram a implementação deste sistema de comunicação anônimo no nível global, afetando ações políticas de grupos públicos e privados. Além disso, em caráter informacional, buscamos descrever a natureza da tecnologia desenvolvida que possibilita o seu funcionamento e efetividade. Esta visão holística do progresso da rede nos permite realizar algumas considerações acerca da estrutura do conhecimento e do "poder" que opera no ciberespaço.

3.3.1 Histórico e Desenvolvimento do 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 HAVENb, 2017).

104 Como os grupos "Omidyar Network" e "The US International Broadcasting Bureau". (DINGLEDINE; MATTHEWSON; SYVERSON, 2007).

Inicialmente, o "The Free Haven Project" pesquisava modos de implementar um sistema capaz de oferecer publicação anônima. Posteriormente, os objetivos passaram a incluir um sistema de comunicação anônimo – e não apenas publicação. Curiosamente, os responsáveis pela implementação, Roger Dingledine[105], Nick Mathewson[106] e Paul Syverson[107] perceberam que, não apenas publicar de modo anônimo era interessante e necessário, mas também manter comunicações via Internet de modo anônimo[108]. O resultado disso é a implementação e lançamento público do software TOR, em 2003, baseado no design de "roteamento cebola" (ou "onion routing") que já era discutido ao final da década de 1990[109]. O software implementou a tecnologia "onion routing" que se assenta sobre o roteamento de fluxos de dados, lidados pelo protocolo TCP, através de "chosen paths in a network of routers using layered encryption and decryption of the content."[110] (PACHENKO; PIMENIDIS; RENNER; 2008, p.221). Cabe lembrar, no entanto, que o software sofreu diversas modificações desde seu lançamento original com o objetivo de implementar melhorias em termos de segurança, eficiência e implantação. (EDMAN; SYVERSON, 2009, p.381).

105 Membro do "The TOR Project". (DINGLEDINE; MATHEWSON; SYVERSON, 2007).

106 Membro do "The TOR Project". (DINGLEDINE; MATHEWSON; SYVERSON, 2007).

107 Membro do "US Naval Research Laboratory". (DINGLEDINE; MATHEWSON; SYVERSON, 2007).

108 Na sequência, o software TOR foi implementado com a possibilidade de comunicação anônima na Internet e, também, navegação anônima na Web.

109 Razão pela qual Dingledine, Mathewson e Syverson categorizam o TOR como parte da terceira geração implantada de designs de "roteamento cebola". (DINGLEDINE; MATHEWSON; SYVERSON, 2007).

110 De modo simplificado: a ideia é que o fluxo de dados são encapsulados em camadas de criptografia. Estas camadas lembram uma "cebola", origem de seu nome. Estes dados, encapsulados em camadas de criptografia, navegam (segundo o protocolo TCP – específico para o controle de transmissão de dados) pela infraestrutura da rede mundial usando um "caminho" que é possível de escolher. Este caminho é escolhido porque, nele, existem roteadores específicos (chamados de "roteadores cebola" ou "onion routers") que são próprios desta rede (que é do tipo "rede roteamento cebola"). A escolha acontece entre quais destes roteadores cebolas utilizar. Por definição, estes roteadores cebolas usam camadas de encriptação e decriptação, ou seja, eles conseguem, remover as camadas de criptografia de cada pacote de dados (as "cápsulas" que envolvem o pacote de dado). (ELAHI et al, 2012, p.43-44). Especificamente sobre os roteadores TOR, *"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). Mais detalhes na seção de funcionamento.

Percebemos, portanto, que o design do "roteamento cebola" se preocupa, essencialmente, com a privacidade e anonimato das informações e dos usuários. Esta primeira noção sobre esquemas de comunicação anônima foi, originalmente, introduzida por Chaum, em 1981[111]. (HOPPER; VASSERMAN; CHAN-TIN, 2010). Neste sentido, o anonimato é definido como sendo

> 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).

No campo cibernético, a preocupação é com a identificação do usuário ou a possibilidade de rastrear suas atividades e, assim, conectar o sujeito à ação. O anonimato sempre foi um assunto dito dicotômico na vida social e no ciberespaço. (LI et al, 2010, p.2). Ele pode ser utilizado para dois fins. Primeiro, pode ser utilizado por um agente que, a depender de suas atividades, confere uma "aura" pacífica, protetora e legítima ou, igualmente, pode ser utilizado de modo a potencializar atitudes e comportamentos ilícitos e criminosos[112]. O advento de novas tecnologias de comunicação proporcionam mercado de estudo e implementação de técnicas que blindem os usuários e as informações de espionagem – uma vez que, atualmente, configura-se a existência de técnicas e ações, de governos e empresas privadas, que objetivam "minerar" a informação que trafega pela massa de usuários da Internet. Em outras palavras, a comunicação na rede mundial de computadores está cada vez menos privada. (MITTAL et al, 2011, p.215). É especialmente ameaçador as invasões de privacidade em potencial de

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)

dissidentes políticos, vazamentos não-oficiais e ativistas políticos – razões pelas quais sistemas de comunicação anônimos estão em voga. (Ibid., p.215). O software TOR, neste sentido, ilumina o caráter político destes tipos de sistema porque confere não apenas anonimato mas também dura resistência à censura. (MOGHADDAM et al, 2012, p.97).

Da necessidade por privacidade, surgem dois nichos no ambiente digital do ciberespaço: os sistemas de "anonimização" e a criação de serviços "anonimizadores". Este último, de acordo com Li et al (2011, p.1) é um produto direto dos sistemas de anonimização (da qual fazem parte as redes de anonimato). Os sistemas de anonimização são sistemas de comunidades contributivas ("community contributed systems") – como o "Java Anon Proxy", o "TOR" e o "I2P". Em comum, eles enviam pacotes de dados através de "relays" ("repetidores") para que nenhum sistema único tenha informações sobre o remetente e o receptor. (Ibid., p.2). Ou seja, formam redes próprias. Já os serviços "anonimizadores" permitem a navegação anônima dos usuários dentro da Web, utilizando um navegador convencional.[113] Cabe lembrar que, neste último caso, pelo fato das empresas que ofertam estes serviços na Web convencional terem a posse de todas as comunicações, elas proveem um grau considerado baixo de anonimato aos clientes.[114] (Ibid., p.5)

O TOR desenvolveu-se com o tempo e tem histórico de melhorias e implementação de novidades técnicas, além de considerável crescimento. Desde sua publicação e lançamento, a comunidade da rede TOR cresceu, atingindo a marca de 1500 roteadores ativos a qualquer momento em 2009. (EDMAN; SYVERSON, 2009, p.385). No site do Projeto TOR, é possível verificar os dados sobre os números de usuários que oferecem suas máquinas como "roteadores" para a rede (de modo a aplicarem o "roteamento cebola") a partir do ano de 2011: neste ano, o número é de menos de 1 milhão, atingindo quase 6 milhões de usuários no segundo semestre de 2013, caindo para menos de 2 milhões no final

113 Estes serviços permitem que o usuário mantenha algum grau de privacidade enquanto navega na Web ao evitar a coleta de informações que possam identificar o usuário como, por exemplo, o endereço de IP da máquina. Tais serviços são providenciados por empresas comerciais, estimuladas pelas taxas de inscrição de usuários, ou organizações não-comerciais que lucram com anúncios ou com serviços elaborados de forma caseira através de ferramentas anônimas de código aberto. (LI et al, 2011, p.1). Alguns destes serviços eram ofertados de modo comercial como o "Anonymizer.com" e "Gotrusted.com". (Ibid., p.5) Para mais informações, verificar LI et al, 2011, p.5.

114 De modo resumido, o grau de anonimato varia pois depende do mecanismo utilizado pelo usuário, das capacidades do adversário que deseja espionar a comunicação e do ambiente da operação. (LI et al, 2011, p.1).

de 2016 e começo de 2017 e, finalmente, superando a marca de 4 milhões ao final de 2017.[115] Desde meados de 2013, o número de usuários é superior a 1 milhão.

Em termos de objetivos, vemos mudanças significativas: no seu princípio, suas metas giravam em torno de duas ideias principais – impedir que ataques pudessem revelar dois agentes que comunicam-se entre si; e impedir que tais ataques também pudessem revelar as várias comunicações "de" ou "para" um único usuário. (CHAABANE; MANILS; KAAFAR, 2010, p.167) Na sequência, o software ganhou popularidade – em especial entre usuários com a intenção de contornar sistemas de censura nacionais como no Irã e na China. (LOESING; MURDOCH; DINGLEDINE, 2010, p.204). De modo lógico, a repressão contra estes usuários foi implementada. Assim, uma das principais inovações que visa, principalmente, atingir usuários em situação arriscada, diz respeito à implementação de "pontes" para acessar a rede TOR. (CHAABANE; MANILS; KAAFAR, 2010). Os esforços comprometidos com o reparo da rede e a implementação de melhorias são contínuos e progressivos. A própria arquitetura da rede tem sido alterada ao longo do tempo de modo a atender estes objetivos. (MOORE; RID, 2016, p.17).

Na próxima seção, nós descreveremos o funcionamento do TOR que permite a privacidade das comunicações e o anonimato entre seus usuários.

3.3.2 Funcionamento do Software TOR

Com o objetivo de compreender o básico do funcionamento TOR, elencamos seis pontos que serão discutidos nesta seção: (1) funcionamento geral, que compreende o tamanho da rede em número de "roteadores cebolas" e comportamento dos usuários; (2) as diferenças entre redes de alta e baixa latência ("high and low latency networks"); (3) o volume de dados "bittorent" e o que isso tem a ver com a rede TOR; (4) por que a rede TOR é uma rede de "aplicação"; (5) o sistema a partir de 3 roteadores-cebola; (6) o papel da criptografia; (7) características gerais. Acreditamos que, se cobrirmos adequadamente os pontos mencionados, será possível entender as razões pelas quais o

115 Verificar ANEXO 6 - "DIRECTLY CONNECTING USERS".

software TOR ganhou popularidade entre os usuários e se tornou uma importante ferramenta política no domínio cibernético do século XXI.

Em termos gerais, talvez a primeira coisa que precisamos saber sobre as redes anônimas é que elas funcionam "escondendo" usuários entre usuários. Isso significa que quanto maior a rede em número de usuários, mais fácil será "misturar" estes usuários entre si de modo que seja mais difícil distingui-los uns dos outros. Em outras palavras, quando novos usuários integram esta rede, os usuários antigos se tornam mais seguros – tudo porque o volume total de usuários cresceu. (DINGLEDINE; MATHEWSON, 2005). Além disso, Dingledine e Mathewson (2005) argumentam que existe mais um "detalhe" para que o anonimato seja possível: os usuários desta rede devem ter comportamentos semelhantes, o máximo possível, para dificultar a distinção entre eles. (Ibid., p.4). É por este motivo que a rede precisa ser acessível para um número razoável de usuários (que sirvam como "roteadores cebola" desta rede) com grau de usabilidade suficiente para que utilizem esta ferramenta sem dificuldades e com propósito semelhante (de modo a extrair deles comportamentos semelhantes). [116]

De acordo com Hopper, Vasserman e Chan-Tin (2010) as redes anônimas se encaixam em duas categorias: as redes anônimas de alta latência e as redes anônimas de baixa latência.[117] As redes de alta latência são, na sua maioria, utilizadas por aplicações do tipo não-interativas com o objetivo de fornecer um forte grau de "anonimato"; e as redes de baixa latência são utilizadas, em larga medida, para navegação anônima e com boa performance na Web. (LI et al, 2010). Ou seja, embora as redes anônimas de alta latência tenham um grau "forte" de blindagem, elas não são utilizadas para navegação e demais aplicações – que são comuns, por exemplo, à navegação da Web na Surface Web. O objetivo da rede TOR é permitir a navegação dos usuários e outras ações derivadas de aplicações voltadas à "navegabilidade" da Web. Por isto, haveria incoerência no desenho da rede TOR caso ela fosse projetada como uma rede de alta latência. Diante disso, a rede anônima TOR é classificada como uma rede anônima de baixa latência, ou seja, prioriza-se além do anonimato a navegabilidade da Web por seus usuários. (DINGLEDINE et al, 2004;

116 Se o objetivo é prover confidencialidade dos dados e armazenamento, deve-se buscar uma rede que dê prioridade a isto. De modo igual, se o objetivo é a privacidade das comunicações, prioriza-se a busca por uma rede cujo objetivo é fornecer isto.

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

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

Em sentido cronológico, primeiro se desenvolveram as redes de alta latência para, na sequência, surgirem as redes de baixa latência. Aquelas primeiras redes fornecem um alto grau de anonimato, mas, em contrapartida, são práticas apenas para aplicações não-interativas que toleram demoras de muitas horas. (EDMAN; SYVERSON, 2009). Alguns destes sistemas de alta latência são o Mixmaster e Mixminion que entregam mensagens após uma demora de cerca de 4 horas em média com o objetivo de garantir anonimato contra um adversário forte capaz de observar o tráfego de dados e controlar alguns roteadores que fazem parte do esquema de anonimato. Por esta razão, as redes de alta latência adotam métodos que resultam na demora na entrega de dados e maior consumo de banda-larga – tudo para "acobertar" o tráfego e dificultar a análise por parte de terceiros. (HOPPER; VASSERMAN; CHAN-TIN, 2010). Isto seria inviável para a rede anônima TOR, visto que ela visa cumprir propósitos de navegabilidade e comunicação dos usuários, ofertando ainda grau de anonimato satisfatório. Seja como for, as redes anônimas de alta latência sofrem "efeitos colaterais", produzidos por esta forte blindagem para prover anonimato, que resultam na demora e consumo de banda. Por isto, as redes de alta latência atraem poucos usuários. (EDMAN; SYVERSON, 2009).

Na sequência, surgem as redes de baixa latência. Elas nascem para suprir a necessidade de melhor performance com o envio dos pacotes de dados em circuitos com pouco atraso de processamento. (MITTAL et al, 2011). As redes que aplicaram a técnica do "roteamento cebola", discutidas por uma literatura desde pelo menos o início da década de 1990, se tornaram as redes de baixa latência mais utilizadas – como a rede TOR e a rede I2P.[118] No que se refere redes de baixa latência, este "design" se tornou o mais adotado. (LI et al, 2010). Além disso, como visto anteriormente, elas são capazes de providenciar uma performance mais rápida e, por isto, são destinadas aos usuários que buscam aplicações interativas e de tempo real, como um chat e

118 Embora ambas utilizem a técnica do roteamento cebola, as redesTOR e I2P são redes diferentes. Sobre isso, Li et al (2010) explica que "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);

navegação da Web, por exemplo.[119] (EDMAN, SYVERSON, 2009; HOPPER, VASSERMAN, CHAN-TIN, 2010; MCCOY et al, 2008; CHAABANE, MANILS, KAAFAR, 2010; LI et al, 2010; AKHOONDI, YU, MADHYASTA, 2012; ALSABAH, BAUER, GOLDBERG, 2012). Esta performance que busca velocidade e interação, no entanto, tem um custo: a resiliência da rede contra alguns tipos de ataques é diminuída, ou seja, há uma redução da garantia do anonimato. (EDMAN, SYVERSON, 2009; HOPPER, VASSERMAN, CHANT-TIN, 2010). De modo mais específico, as redes de baixa latência são mais suscetíveis à análise de tráfego de dados por um adversário capaz de observar a conexão do usuário com a rede e a conexão da rede com o destino pretendido pelo usuário. (EDMAN; SYVERSON, 2009). Em outras palavras, enquanto as redes de alta latência fornecem forte grau de anonimato e degradação da experiência de atividade do usuários, as redes de baixa latência ofertam justamente o contrário.

Outra característica das redes de baixa latência é a navegabilidade utilizando "janelas" de navegação da Web. Esta "janela", na realidade, é o navegador próprio da rede e permite também compartilhamento de arquivos, troca de mensagens instantâneas, etc. – bem próxima da funcionalidade de um navegador convencional. [120] (MCCOY et al, 2008). A rede TOR preocupou-se especialmente com a experiência de interatividade do usuário e alcançou a popularidade, sendo a ferramenta mais utilizada no que tange as tecnologias de anonimato. (AKHOONDI, YU, MADHYASTHA, 2012; LI et al, 2010).

Mas atrasos também acontecem na rede TOR. Menores que os atrasos das redes de alta latência, mas eles existem e às vezes duram segundos – o que afeta a qualidade de navegação, por exemplo. (DUNGHEL et al, 2010). Os principais contribuintes para a demora são os atrasos referentes aos roteadores – cerca de 11% ou mais dos roteadores da rede estavam sobrecarregados com tráfego de dados em

119 Essa capacidade é possível porque estas redes buscam, ativamente, limitar o atraso do processamento e a sobrecarga da largura de banda. (HOPPER; VASSERMAN; CHAN-TIN, 2010, p.3)

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). Ou seja, houve uma decisão política em reduzir a latência para alcançar o objetivo de navegação da Web dentro da rede TOR. A navegação da Web não é abrangida pelas redes de alta latência. A rede TOR depende de uma rede sobreposta, distribuída e que utiliza a tecnologia de "roteamento cebola" para tornar anônimo os aplicativos da camada TCP (aplicativos interativos como a navegação, encapsulamento de dados, comunicações peer-to-peer). (CHAABANE, MANILS, KAAFAR, 2010).

2010. E ele não são os únicos que contribuem para a demora de resposta da rede. (Ibid., p.4). Na verdade, o tráfego de dados na rede TOR não é distribuído de modo uniforme entre os vários circuitos.[121] Um número baixo de circuitos é responsável por consumir uma quantidade desproporcional de largura de banda e o maior responsável é o BitTorrent. (ALSABAH; BAUER; GOLDBERG, 2012). Apesar da navegação na Web corresponder a 92% de todas as conexões TCP da rede TOR, esta navegação corresponde a apenas 60% do volume de dados que trafegam na rede. Os outros 40% são do volume de dados são atribuídos ao BitTorrent.[122] (ALSABAH; BAUER; GOLDBERG, 2012). Isso significa que o BitTorrent é um dos protocolos mais utilizados na rede TOR – o que levou Chaabane, Manils e Kaafar (2010, p.174) a afirmar que o tráfego do tipo P2P ("peer-to-peer"), como o BitTorrent, não está desaparecendo da Internet mas apenas se escondendo em canais criptografados, como dentro desta rede anônima. Em outras palavras, o BitTorrent é responsável pela degradação da rede TOR. Sobre isso, Johnson et al (2013) afirma

> 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).

Os usuários que utilizam o BitTorrent pela rede TOR também são os "menos" anônimos porque suas atividades não se relacionam com a navegação da Web, como os demais usuários. Esta distinção de operações torna este grupo um "destaque" na rede, ou seja, são mais evidenciados. Portanto, além de serem responsáveis pela degradação da rede, tornando-a mais lenta para os usuários que a utilizam para navegação, os usuários BitTorrent estão menos protegidos que os

121 Circuitos são os caminhos ("paths") pelos quais os dados percorrem dentro da rede TOR, desde o remetente até o destinatário. Quando um dado é enviado, ele não circula por todos os roteadores da rede: ele caminha pelo circuito estabelecido entre alguns dos roteadores. Ou seja, dentro do universo de roteadores cebola da rede TOR, o circuito é um conjunto pré-selecionados deles que fornecem o caminho pelo qual o dado caminha na rede.

122 Em 2010, acreditava-se que o volume de dados de BiTorrent trafegados na rede TOR correspondia a mais da metade, o que gerava danos ao tráfego geral de dados por forçar o aumento da latência da rede e reduzir a rapidez. Ou seja, a maior parte dos dados que navegavam na rede TOR eram dados criptografados de BitTorrent. (CHAABANE; MANILS; KAAFAR, 2010, p.170).

demais. As constantes melhores e implementações na performance da rede TOR como um todo são essenciais para a manutenção do grau de anonimato, da usabilidade de navegação e proteção da privacidade dos usuários que compõem esta rede de baixa latência. (ALSABAH; BAUER; GOLDBERG, 2012).

Em termos de funcionamento técnico, talvez nada seja mais importante que compreender o sistema da rede TOR baseada no princípio dos "três roteadores". Na literatura sobre o assunto, sem sombra de dúvidas, é o elemento técnico mais amplamente descrito. (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). Este modelo de funcionamento baseado no princípio dos três roteadores também é conhecido como princípio dos três nódulos. Neste ponto, é importante relembrar como os pacotes de dados viajam pela malha da rede muncial de computadores – como imaginado e pretendido por Paul Baran, responsável por criar a tecnologia de comutação de pacotes – porque existem diferenças. E estas diferenças de como os pacotes viajam e são transmitidos são fundamentais para compreender, pelo menos parcialmente, de que modo as redes anônimas são regiões distintas da rede mundial de computadores.

A rede TOR é composta por inúmeros servidores únicos chamados de "roteadores cebolas" (Onion Routers, OR). (PACHENKO; PIMENIDIS; RENNER, 2008). Estes servidores, ou melhor, roteadores cebolas, são computadores voluntários que formam a rede e estão distribuídos em diferentes localidades do mundo. É a partir deste oceano de computadores voluntários que um usuário qualquer cria um "caminho", também chamado de "circuito", por meio do qual sua mensagem irá percorrer. Este caminho é formado por nódulos (computadores voluntários). (EDMAN; SYVERSON, 2008).

O primeiro passo é executar um Onion Proxy (OP) que nada mais é do que um software que separa a rede local da rede externa.[123].

123 Definição de Proxy é dada a seguir: "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).

(PACHENKO, PIMENIDIS, RENNER, 2008; DUNGHEL et al, 2010; LI et al, 2010; ELAHI et al, 2012). Ou seja, este software é responsável por tornar a máquina do usuário parte integrante da rede anônima de baixa latência TOR. O próximo passo é criar um circuito, a partir dos OR's disponíveis – que são os computadores voluntários que formam a rede. Por padrão, o número de roteadores escolhidos é três.[124] (MCCOY et al, 2008). Juntos, estes três roteadores fornecem o caminho para o envio e recebimento de dados – e este é o circuito pelo qual os dados são encaminhados. Os dados são "encapsulados" de acordo com a estratégia de criptografia em camadas – típica do "roteamento cebola" – e em seguida percorrem o circuito estabelecido. (Ibid., p.64).

O usuário da rede inicia a sessão pelo primeiro nódulo do circuito. Este primeiro nódulo é chamado de Entry Node (ou "nódulo de entrada"). Ele é conectado ao segundo nódulo, chamado de Middle Node ("nódulo intermetdiário), através de um túnel criptografado que é estabelecido entre os dois nódulos. Na sequência, o Middle Node é conectado ao terceiro nódulo, conhecido como Exit Node (ou "nódulo de saída"), também através de um túnel criptografado.[125] Este túnel criptografado resultado da conexão destes nódulos é conhecido como "circuito" – caminho pelo qual os dados encapsulados percorrem. (EDMAN; SYVERSON, 2009, p.381; MCCOY et al, 2008, p.65). Cabe lembrar que o número padrão de nódulos é três mas pode ser estendido, até quanto possível, pelo usuário.

Como dito anteriormente, as mensagens são criptografadas de acordo com o esquema típico do "roteamento cebola": a mensagem inicial é criptografada "n" vezes ("n" corresponde ao número de nódulos

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). Tipicamente o número de roteadores selecionados pelo usuário são três mas nada impede que o número seja outro. Estes roteadores também são comumente chamados de nódulos. (EDMAN, SYVERSON, 2009; CHAABANE; MANILS, KAAFAR, 2010; DUNGHEL et al, 2010). Caso deseje um circuito com mais de três roteadores, ou nódulos, o usuário deve realizar o download de uma lista destes (com alguma informação adicional). Nesta lista, existe a indicação de "status flag" de cada nódulo disponível (cuja condição no momento é considerada pelo usuário durante a sua escolha). O usuário escolhe três nódulos ativos (estes são chamados de "guardas") que servirão de porta de entrada para os demais circuitos a serem construídos. Os "guardas" são rotacionados de modo dinâmico em um período de 30 a 60 dias – para não serem estáticos e "presas" fáceis aos adversários da rede. (JOHNSON et al, 2013, p.338).

125 Este terceiro e último nódulo é chamado de "nódulo de saída" porque é responsável por estabelecer uma conexão da rede TOR com o destino final pretendido pelo usuário. (EDMAN; SYVERSON, 2009).

do circuito). Se existem três nódulos no circuito, a mensagem é criptografada três vezes, por exemplo. A primeira camada de criptografia apenas pode ser lida pelo último nódulo, Exit Node. Este último nódulo detém a chave criptográfica para ler a primeira camada. O penúltimo nódulo é capaz de ler a segunda camada criptográfica. O antepenúltimo nódulo é capaz de ler a terceira camada criptográfica. E assim sucessivamente. Esta é a razão deste esquema criptográfico ser conhecido como "cebola", pois a mensagem é envolta por diferentes camadas e cada nódulo do circuito estabelecido apenas consegue decifrar uma única camada de criptografia. Por este motivo, cada nódulo intermediário sabe apenas sobre o nódulo anterior e posterior a si próprio – ou seja, nenhum nódulo é capaz de reconhecer todos os nódulos do circuito. (CHAABANE, MANILS, KAAFAR, 2010, p.167; AKHOONDI, YU, MADHYASTHA, 2012). Na prática, cada nódulo do circuito é capaz de remover apenas uma única camada de criptografia do pacote de dados e encaminhar para o próximo nódulo. (DUNGHEL et al, 2010; HOPPER, VASSERMAN, CHAN-TIN, 2010; LOESING, MURDOCH, DINGLEDINE, 2010). Sendo assim, apenas o nódulo de entrada é capaz de observar o originador de um pedido específico através da rede TOR – da mesma forma que apenas o nódulo de saída é capaz de identificar a mensagem, remover a última camada criptográfica do pacote de dados e conhecer o destino final. Ou seja, não há como um único roteador dentro do circuito saber as identidades do usuário e do destinatário do circuito, uma vez que cada roteador conhece apenas o "micro universo" composto de si próprio, predecessor e sucessor. (MCCOY et al, 2008; DUNGHEL et al, 2010). A resposta, que parte do destino final em direção ao usuário da rede, também utiliza o mesmo processo do roteamento cebola de criptografia: a mensagem do destino final é criptografada em camadas e decifrada pelo usuário. (LOESING; MURDOCH; DINGLEDINE, 2010). Este pacote de dados, resposta do destino final ao usuário da rede, é roteado através dos mesmos três nódulos da mensagem original – mas no sentido contrário. (DUNGHEL et al, 2010). Cabe lembrar ainda de um detalhe: muitos usuários da rede TOR utilizam os mesmos nódulos intermediários ao mesmo tempo, de modo que a conexão de Internet de qualquer um destes usuários está "escondida" no meio de outras conexões de outros usuários, o que torna cada sistema individual inviável de ser atrelado a um usuário específico. (LI et al, 2011, p.2). Por todas estas razões, a rede de baixa latência

TOR, que utiliza a tecnologia "roteamento cebola", é dita uma rede anônima.[126]

A equipe que mantém a rede TOR ativa, conhecida como Tor Project, elaborou um mecanismo capaz de contornar ações de governos que buscam bloquear as conexções à esta rede anônima. Este mecanismo é conhecido como "bridges" ("pontes"). (LOESING; MURDOCH; DINGLEDINE, 2010). O problema, originalmente, acontece quando os Internet Service Providers (ISP), também conhecidos como Provedores de Serviço de Internet, empresas responsáveis por conectar os dispositivos do usuário à rede mundial de computadores, bloqueiam o acesso à rede TOR ao filtrar os endereços de IP dos nódulos do circuito. Como um modo de contornar este bloqueio, o Tor Project criou as "bridges". Funciona da seguinte forma:ao conectar a sua máquina à rede TOR, por meio do Onion Proxy, o usuário tem a opção de escolher três nódulos, ou mais, para criar o circuito que utilizará. As opções de nódulos são fornecidas em uma lista de roteadores disponíveis (esta lista está no "TOR Directory").[127]Estes nódulos "públicos" do diretório TOR (pois qualquer usuário pode ter acesso) podem ser bloqueados pelos provedores de serviço de internet. Assim, àqueles que desejam conectar-se à rede anônima TOR mas encontram-se, por algum motivo, impedidos podem solicitar uma "bridge" ao Tor Project. Esta "bridge" é uma alternativa de acesso à rede anônima (àqueles que não podem selecionar nódulos dispostos no diretório público). O Tor Project fornece três "bridges" ao usuário pedinte por um período fixo de tempo. Como estas "pontes" não estão listadas no diretório público e existem por um tempo limitado, torna-se difícil sua localização e consequente bloqueio. (CHABAANE, MANILS, KAAFAR, 2010; LOESING, MURDOCH, DINGLEDINE, 2010). No entanto, Moghaddam (2012) ressalta a efetividade das "bridges" sem deixar de admitir que ainda há meios de bloqueá-los: como qualquer usuário pode pedir acesso às

126 Uma das características da rede TOR é a possibilidade de navegação da Web através do navegador de mesmo nome, "TOR Browser". Ao invés dos endereços nominais das páginas serem listadas com terminações do tipo ".com" ou ".org" ou ".net", elas são terminadas com o sufixo ".onion" – característico do TOR. Além disso, este endereço é dinâmico, alterando-se a cada requisição de visita. (MOORE; RID, 2016, p.18).

127 Para mais informações sobre o diretório TOR com a listagem de nódulos através do Onion Proxy, consultar: 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. Para consultar o funcionamento técnico da rede TOR em mais detalhes, especialmente sobre a criação de circuitos, verificar ELAHI et al, 2012, p.43-45.

"bridges", é possível descobrir seus endereços de IP. Além do mais, as técnicas de censura sofrem melhorias e novas implementações com o tempo e, assim, novos métodos são implantados para descobrir e bloquear estas "bridges" ofertadas pelo Tor Project.

Ainda sobre possíveis "falhas" da rede TOR, que podem, em algum momento, rebaixar ainda mais o grau de anonimato conferido por esta rede de baixa latência, Johnson et al (2013) nos lembra que os usuários da rede devem realizar considerações sobre suas próprias necessidades de segurança – visto que a rede oferece menor grau de anonimato em troca de maior usabilidade e aplicabilidade (ao contrário das redes de alta latência). Existe o risco de infiltração também: por exemplo, um usuário da rede que tenha voluntariado sua máquina para ser um roteador cebola com maior largura de banda. Em 2013, Johnson et al, realizou um estudo em que constatou que existe a possibilidade de 50% de um usuário identificar os demais dentro de um período médio de até 3 meses. Em até 6 meses, esta probabilidade de identificação cresce até 80%. (JOHNSON et al, 2013, p.337). Sobre isto, Moore e Rid (2016) oferecem segurança quando afirmam que

> 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)

Ou seja, apesar de existir a possibilidade de "des-anonimar" o usuário, a implementação cuidadosa de alguns procedimentos básicos fornecem a robustez necessário para que o sistema de comunicação permaneça seguro e projeta o anonimato dos usuários e a privacidade das comunicações. O software TOR demonstra ser uma relevante ferramenta no domínio cibernético, com adequada usabilidade e funcionamento de razoável compreensão por parte dos usuários que planejam utilizá-lo como sistema de navegação da Web e demais comunicações interativas.

Na sequência, nosso objetivo é descrever o surgimento dos "serviços ocultos" oriundos da rede TOR que, com frequência, recebem o nome de "darknet" por operarem nos termos de um mercado negro,

com inúmeros produtos e serviços considerados ilícitos, dentro da rede anônima de baixa latência. Sem dúvidas, o sucesso dos serviços ocultos se dá, em larga medida, pela utilização robusta de técnicas de criptografia – o que levou os pesquisadores Daniel Moore e Thomas Rid (2016) a considerarem as políticas que envolvem a criptografia um relevante tema de discussão acadêmica para o século XXI.

3.3.3 Os Serviços Ocultos ("Hidden Services")

O software TOR permite tanto a navegação anônima na Surface Web, como na Dark Web.[128] A maioria dos usuários que utilizam o software TOR para navegar na Surface Web de modo mais seguro ou anônimo.[129] (MOORE; RID, 2016). No entanto, como vimos, é possível interagir dentro da rede e acessar as páginas ocultas nos endereços ".onion". Desta lógica, surgem os "serviços ocultos" da rede TOR, como atestam Moore e Rid (2016):

> 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.

128 Na página do Tor Project, na web superficial, é possível observar a listagem de softwares e serviços ofertados pelo projeto que, até novembro de 2017, incluíam: "Tor Browser", navegador seguro de navegação da Internet; "Nyx", terminal que mostra o status da rede TOR; "Metrics Portal", ciências de análise da rede TOR; "Tor Messenger", plataforma de mensagens instantâneas que opera na rede TOR; "Pluggable Transports", que transforma o tráfego de dados da rede TOR entre o usuário e a "ponte" ("bridge"), de modo a contornar censores e bloqueios; "Onionoo", protocolo baseado na Web que instrui-se sobre roteadores da rede TOR e as "pontes"; "Orbot", plataforma do TOR no sistema operacional android; "Shadow", simulador da rede TOR que executa o software para experiências (especialmente para desenvolvedores abertos); "Stem", conjunto de termos da linguagem computacional Python para aplicações e programas que interagem com o TOR; "Tails", sistema alocado em portas USB's (como um pen-drive ou "HD externo") pré-configurado para usar a rede TOR e não deixar rastros no sistema local; "Tor Birdy", extensão do Mozilla Thunderbird; "Txtorcon", implementações da linguagem Python e Twisted sobre o protocolo de controle do TOR; "Ooni", rede global de observação que busca coletar dados de alta qualidade utilizando metodologias abertas ("Free and Open Source Software") para compartilhamentos sobre os diferentes tipos de quantidades, métodos e tipos de adulterações na rede globalmente. (TOR PROJECT, 2017).

129 Software TOR é um programa que permite o acesso à rede anônima de mesmo nome mas que também oferece outras aplicabilidades.

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

Estes serviços ocultos ("Hidden Services") são responsáveis por 3-6% de todo o tráfego da rede TOR.[130] As pesquisas apontam que o uso mais comum destes serviços são de caráter criminoso: envolvem desde o comércio de drogas até a pornografia que envolve crianças e animais. (Ibid., p.16). Moore e Rid (2016) salientam ainda a "fama" dos serviços ocultos da rede TOR na Rússia: a poderosa organização de censura, Russia's Safe Internet League, e o secretário de imprensa, regulador da mídia do Kremlim, Vadim Ampelonsky, descrevem a rede TOR como um ambiente em que se tolera diversas ações ilícitas que permite o esconderijo de criminosos das autoridades russas. Os serviços ocultos dão um nome ruim à rede TOR e às tecnologias criptográficas no geral. Curiosamente, apesar de ser projetado para não deixare rastros, nenhum dos criadores originais mencionou os mercados ilícitos, um serviço oculto que surgiu como consequência da arquitetura do sistema da rede e das páginas ocultas. (Ibid., p.27).

Diante da tecnologia criptográfica, da rede anônima e dos serviços ocultos, uma miríade de atores surge com os mais diversos objetivos: extremistas islâmicos, comunidades criminosas, lavagem de dinheiro, oferta de drogas e entorpecentes, pornografia infantil e de animais, hacking, violência, etc.[131] Alguns pontos relevantes oriundos do estudo de Moore e Rid (2016) são: a quase ausência de conteúdo extremista islâmico nos serviços ocultos da rede TOR[132]; comunidades criminosas online tendem a migrar para a rede TOR devido aos seus recursos de segurança e anonimato; a lavagem de dinheiro é recorrente e

130 O termo "darknet", empregado pelos pesquisadores Daniel Moore e Thomas Rid, por exemplo, se refere a este conjunto específico de páginas e serviços ocultos por meio de criptografia – como vimos anteriormente ao discutirmos a definição de "Dark Web". (MOORE; RID, 2016, p.15).

131 Para mais informações, conferir "Anexo 6 - Classification".

132 Ao que tudo indica, existem algumas páginas ocultas da rede que estavam ativas em 2016, época da pesquisa, mas um número pequeno. Os extremistas preferem utilizar a internet de dois modos: atividades para o público (propaganda, recrutamento e compartilhamento de sugestões) e atividades escondidas do público (comunicação interna e comando e controle). (MOORE; RID, 2016, p.21). Inclusive, o Estado Islâmico (ISIS) possui uma página destinada à propaganda no serviço oculto da rede TOR, lançada em novembro de 2015. (Ibid., p.29).

a moeda mais utilizada é o Bitcoin; a comodity mais comum da rede TOR é a droga, seja ela de vários tipos. Se é verdade que muitas ações criminosas e conteúdos ilícitos encontram na rede anônima de baixa latência, então é razoável supor que existe crescente dificuldade para a disciplina de Forense Digital ("Digital Forensics") – que surgiu como área na década de 1980, com os primeiros indícios de crimes virtuais, e tem tido relevante destaque na detecção e prevenção de crimes digitais. (HORSMAN, 2017, p.448). Na prática, as evidências oriundas da Forense Digital são utilizadas em tribunais de justiça para dar apoio ao sistema da justiça criminal. No entanto, desde 2010 vem se discutindo a efetividade da disciplina enquanto debate-se se a era de ouro da Forense Digital estava no fim. Alguns afirmam que existe evidência suficiente para afirmar que isto é uma verdade devido aos grandes desafios enfrentados pela área diante da natureza tecnologicamente criptográfica de muitos softwares e técnicas digitais. Uma dessas evidências é a proliferação dos mercados anônimos digitais provenientes dos serviços ocultos das redes anônimas, como o TOR.(Ibid., p.449).

No entanto, Roger Dingledine, um dos criadores do TOR, nega a relevância dos "serviços ocultos" dentro da plataforma da rede. (THOMSON, 2017). Suas críticas giram em torno da desinformação proferida por jornalistas que, segundo ele, misturam os "serviços ocultos" da rede, em que apenas 3% dos usuários utilizam, com a simples navegação anônima da Web. Segundo Thomson (2017), para Dingledine, estes serviços ocultos (que ele chama de Dark Web[133]) são insignificantes[134].

Originalmente, o "serviços oculto" tiveram início na década de 1990 com o "BlackNet". Atualmente, as redes de serviços ocultos utilizam software para permitir acesso às redes distribuídas, cujos maiores exemplos são as redes TOR, I2P e Freenet. (MOORE; RID, 2016, p.7). Em especial, os seviços ocultos da rede TOR combinam duas características específicas, como salientam Rid e Moore (2016):

133 Dingledine não faz diferenciação entre os termos da literatura sobre o assunto. No contexto mencionado, fica evidente que, para ele, os "serviços ocultos" da rede TOR e a própria "Dark Web" são a mesma coisa.

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).

> 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).

Em outras palavras, os serviços ocultos ofertados por meio de servidores não estão protegidos, especificamente, pela rede TOR (embora a comunicação e as localizações físicas entre os agentes que se comunicam pela rede sim) mas pelos provedores de acesso à internet, que possuem a capacidade de determinar em que endereço, da malha da Internet, está localizado o servidor. De qualquer modo, os criadores originais da rede TOR reconhecem os serviços ocultos da rede e ainda buscam usos adequados e apropriados para estes serviços. (Ibid., p.29).

3.3.4 O Papel da Criptografia

Talvez o mais curioso seja o fato de os protocolos criptográficos, que sustentam os serviços ocultos de modo geral, eram considerados ameaças até por volta de 1995. (Ibid., p.28) Em um ambiente cibernético calcado na cultura da liberdade e fluxo de informação desenfreado, os protocolos criptográficos surgiam como obstáculos para terceiros interessados na comunicação livre entre dois agentes. Não por isso, Moore e Rid (2016) afirmam que a política em torno da criptografia é um teste crucial dos valores da democracia liberal do século XXI: enquanto o poder criptográfico confere proteção aos cidadãos em suas atividades de compras online, leitura, acesso aos bancos, este mesmo poder pode proteger indivíduos mal-intencionados. A criptografia é o elemento central das maiores ameaças da nossa era – extremismo militante e brechas nos sistemas de informação – ao mesmo passo que provê prosperidade e privacidade. (Ibid., p.7). A esta onda conflitante de posicionamentos relativos às políticas em torno da criptografia convencionou-se chamar de "Cryptowars", cuja origem é datada do início da década de 1990 com o debate em torno do chip

"Clipper". [135] Em suma, as "Cryptowars" são debates tecnológicos sobre o posicionamento do governo em acessar comunicações criptografadas, ou não, e envolve atores de segurança nacional, empresas tecnológicas e usuários da Internet. (SCHULZE, 2017). A criptografia é o elemento de destaque nos debates que envolvem o domínio cibernético e a política no início do século XXI. Além disso, é parte do eixo técnico central por trás da rede anônima de baixa latência TOR – como vimos anteriormente. Por esta razão, é importante compreender o que é a criptografia e quais são as suas propriedades.

A criptografia nada mais é do que uma técnica de "misturar" texto legível, utilizando algoritmos matemáticos, em um texto cifrado e ilegível. (SCHULZE, 2017). Buchanan (2017) explica que "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). Ou seja, o objetivo da criptografia é manter uma determinada informação sigilosa para terceiros, enquanto perfeitamente compreensível para os indivíduos destinados a conhecer a informação. O problema, no entanto, é o seguinte: como o indivíduo A, que cifrou a mensagem utilizando uma determinada chave, pode informar esta chave para o indivíduo B, que a usará para decifrar a mensagem? Esta questão é conhecida como o "problema da distribuição de chave" (ou "the key-distribution problem"). Este problema é particularmente grave no setor militar,

135 O início das chamadas "Cryptowars" é em 1992, quando a empresa de comunicação estadunidense American Telephone and Telegraph (AT&T) inicia o desenvolvimento de um telefone capaz de criptografar a comunicação por voz entre dois indivíduos. A proposta era a utilização de um chip chamado "Clipper" que seria anexado aos equipamentos eletrônicos como telefones e computadores – e uma cópia da chave criptográfica (Encryption Key) seria guardada em bancos de dados do governo. Esta chave, na prática, permitia o acesso livre do governo. O debate continuou até o ano de 1995, quando a proposta da empresa foi deixada de lado. O General Michael Hayden, dos Estados Unidos, chegou a afirmar que a NSA perdeu esta batalha afirmando "We didn't get the Clipper Chip, we didn't get the back door." (SCHULZE, 2017, p.55). O debate é retomado no novo milênio, em 2014, quando a empresa tecnológica Apple decidiu implementar padrões criptográficos nos seus celulares, o que gerou uma discussão que envolveu o então diretor do FBI, James B. Comey, e o CEO da Apple, Tim Cook. Ambos estiveram no centro do debate: enquanto Comey insistiu que o governo adotasse medidas legislativas sobre o assunto da criptografia nos aparatos tecnológicos, Cook argumentou que esta ação era excessivamente onerosa. O debate prosseguiu até o ano seguinte quando uma corte de justiça do Brooklyn, EUA, decidiu em favor da Apple. (Ibid., p.56). De modo resumido, o debate é dividido em duas grandes vozes: aqueles que acrediam que as tecnologias criptográficas são benéficas e aqueles que afirmam o contrário. (Ibid., p.57; MOORE, RID, 2016, p. 8).

chegando a afetar o uso tático do rádio. (MOORE; RID, 2016, p.10). Em 1976, a solução para o problema foi desvendada: a solução seria adotar o método da "chave pública" (ou "public-key"). (SCHULZE, 2017). Este é o marco da criptografia moderna. De acordo com 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). A solução para o problema é manter a chave em modo público.[136]

Para Moore e Rid (2016), o conceito por trás da chave-pública foi uma das invenções pivôs de todo o século XX pois permitiu a recriação, e a melhoria, dentro do contexto eletrônico, das cinco propriedades fundamentais da comunicação humana: (1) privacidade, um modo de proteger as mensagens (especialmente em trânsito) contra o acesso não-autorizado do conteúdo; (2) autenticação, a maneira de identificar que a mensagem tem origem do remetente específico; (3) anonimato, o modo de esconder a identidade do autor tanto do destinatário quanto outros observadores; (4) cédula de dinheiro, que não tem identidade e são anônimas; (5) trocas ocultas, que é a possibilidade de realizar trocas e criar mercados através das quais as transações são seguras, autenticadas e anônimas. (MOORE; RID, 2016, p.11-14). Os serviços ocultos das redes anônimas recriam, com a ajuda da criptografia, o ambiente para estes espaços proliferarem: estes mercados ocultos possibilitam as trocas de bens e serviços, lícitos e ilícitos, em uma forma melhorada – no domínio cibernético. (Ibid., p.14). Para os autores,

> 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).

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).

A criptografia, atualmente, faz parte de um conjunto específico de técnicas que estão sedimentadas na cultura da Internet. Em especial, ela tem impacto relevante na Dark Web, seja por meio da rede anônima de baixa latência TOR, seja por alguma outra rede anônima como a Freenet e a I2P. Cabe ressaltar, contudo, que os posicionamentos do debate acerca do assunto é amplo: de um lado, atores públicos que versam sobre os perigos oriundos do uso de criptografia nos equipamentos eletrônicos; do outro, atores privados que enaltecem os valores de liberdade, privacidade e segurança que são conferidos por tais mecanismos no domínio cibernético. As chamadas "Cryptowars" são eventos recorrentes e inconclusivos. Os serviços ocultos da rede TOR, apesar de não terem sido projetados intencionalmente por seus criados, são um fenômeno derivado das quatro propriedades da criptografia. (Ibid., p.28). Por esta razão, hoje tornou-se possível realizar compras e manter comunicações privadas, dentro do domínio cibernético, de modo a manter-se oculto do vendedor, autoridades do imposto de renda, da aplicação da lei ou demais terceiros. (Ibid., p.14).

3.3.5 Popularidade e Política

É dito que a rede TOR é o sistema de comunicação anônimo mais empregado da era atual, tornando-se o mais popular e difundido método. (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). A rede ganhou alguma notoriedade em 2004, quando tinha cerca de 2 mil nódulos de roteadores voluntários – chegando a mais de 250 mil nódulos em 2009. (EDMAN; SYVERSON, 2009, p.380). Este ganho em termos de número de nódulos é benéfico para a rede porque quanto mais roteadores houver disponível, mais difícil é distinguir os usuários ao realizar-se análise de tráfego da rede. O aumento do número de roteadores aumenta a capacidade da rede de gerir simultaneamente os usuários, além de diminuir a quantidade de tráfego observado por um adversário que controla alguns dos nódulos. (Ibid., p.388). Uma das razões da popularidade do TOR é sua técnica de implementação de anonimato que combina partes de métodos anteriores eficientes, como o diretório de roteadores para uso do usuário, o estabelecimento de circuitos telescópicos e os locais escondidos. (LI et al, 2011, p.6). Além

disso, a rede TOR tem uma base de voluntários mais estável que a rede anônima I2P – e em termos absolutos, seu número de voluntários também é maior. (Ibid., p.31). As redes anônimas, afinal, são bastante procuradas por usuários interessados em privacidade e anonimato. (CHAABANE; MANILS, KAAFAR, 201).

Se no início os usuários da rede eram entusiastas técnicos, à medida que o projeto foi ganhando notoriedade e reconhecimento, novos usuários, com poucas habilidades técnicas, foram integrando a rede. O software foi tema de conferências de segurança, artigos de revistas técnicas e meios de comunicação tradicionais – como os jornais The New York Times e Wall Street Journal, e a revista norte-americana Forbes. (DINGLEDINE; MATHEWSON, 2005). De fato, a rede é utilizada por diferentes atores sociais: de cidadãos privados, passando por empresas e chegando até os governos – e por razões que variam desde a proteção das comunicações virtuais até o contorno de sistemas de censura. (LOESING; MURDOCH; DINGLEDINE, 2010). Tem também sido considerado um serviço crucial para ativistas do governo, jornalistas, empreendimentos, empresas e setores militares. (MITTAL et al, 2011, p.215). Quanto mais a rede se torna popular entre as massas, mais intenso é o esforço de governos em conter seu uso. Inclusive, a EFF já se posicionou a favor da rede, oferecendo assistência aos usuários de roteadores voluntários que receberam notificações do governo norte-americano por meio da Digital Millenium Copyright Act (DMCA) para retirar seus roteadores da rede. (MCCOY et al, 2008). Outros atores que se posicionaram a favor do TOR incluem o gigante Google e a organização Human Rights Watch que advoga pela navegação através da ferramenta e recomenda o uso para dissidentes, como uma forma de contornar medidas governamentais de repressão. (MOORE; RID, 2016, p.17). Em outubro de 2017, o jornal The New York Times adotou a plataforma para oferecer seus serviços.[137] (SANDVIK, 2017).

Em 2008, o alcance da rede TOR abrangia cerca de 126 países, evidenciando seu apelo global – com destaque para os países da

137 "The New York Times reports on stories all over the world, and ourreporting 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).

Alemanha, China e Estados Unidos.[138] (MCCOY et al, 2008; LI et al, 2011). A rede anônima e o projeto TOR, enfim, ganharam contornos nitidamente políticos. Em 2010, escrevendo conjuntamente com Loesing e Murdoch, um dos criadores do TOR, Roger Dingledine, admitiu que o propósito da rede TOR é oferecer anonimato e contorno à censura para as pessoas ao redor do mundo: "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). Chabaane, Manils e Kaafar (2010) complementam, afirmando que "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).

De fato, a rede TOR permite não apenas privacidade nas comunicações mas também meios de contornar a censura imposta em alguns Estados e resistir a vigilância na Internet. Este aspecto da rede TOR permite que usuários residentes em países opressivos e/ou autoritários tenha acesso à informação sem medo de represálias como o bloqueio, o rastreamento ou a monitoração de suas atividades online.[139] (ALSABAH; BAUER; GOLDBERG, 2010). Por exemplo, se o usuário reside em um país autoritário que determina a censura de páginas da Web, ele pode recorrer à rede TOR para contornar esta censura e ter acesso ao conteúdo das páginas censuradas – basta requisitar o conteúdo censurado que será entregue a ele. (MOGHADDAM et al, 2012, p.97).

Existem tantos exemplos na literatura em relação ao uso político da rede TOR em diferentes nações quanto existem de tentativas de bloquear o seu uso por parte destas mesmas nações. O uso do TOR em número de usuários, por exemplo, aumentou significativamente no espaço cibernético do Irã a partir de 2009 – após as eleições iranianas. A rede TOR é destaque na China e desde setembro de 2009 o governo

138 É importante compreender de onde surgem estes dados. Sobre isso, destacamos a literatura de 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 De acordo com Alsabah, Bauer e Goldberg (2010) há evidências do sucesso da rede TOR: o número de downloads do software e o crescimento de usuários na rede são indicativos do seu caráter revolucionário e de sua força na luta política e social das realidades destes usuários; sendo uma influente tecnologia anti-censura.

chinês bloqueou o acesso à maioria dos roteadores-cebolas da rede.[140] Por esta razão, o número de "bridges", no momento posterior ao bloqueio, aumentou em 70%. (LOESING; MURDOCH; DINGLEDINE, 2010, p.206). No Egito, em 2011, milhares de indivíduos fizeram o download do software TOR para comunicação e disseminação de informações – mesmo após a forte repressão à Internet movida pelo regime de Mubarak. Outro destaque é relativo aos rebeldes do conflito da Síria: eles foram capazes de expor evidências digitais das atrocidades, cometidas pelo regime de Bashar Al-assad, sem expor a identidade daqueles que conseguiram reunir as evidências. (MOORE; RID, 2016). As tentativas de bloqueio são pelos provedores de acesso à Internet e são feitas no nível local e regional: como a lista do diretório geral dos roteadores-cebola da rede é aberta e pública, o bloqueio à rede pode ser feito bloqueando o acesso de todos os roteadores desta lista com base nos endereços de IP (para localizá-los no endereço da malha da Internet). (MOGHADDAM et al, 2012). É por esta razão que existem roteadores alheios a esta listagem – são as "bridges".[141] Contudo, cabe lembrar que as "darknets" não são ilegais nos países livres. (MOORE; RID, 2016, p.32).

Concluímos por aqui o conjunto de informações sobre a rede TOR necessárias para a compreensão das razões que a fazem uma ferramenta de combate à censura e forte aliada da privacidade dos usuários.

3.4 A ESTRUTURA DO CONHECIMENTO NO SÉCULO XXI

140 Este fenômeno de bloqueio está atrelado à política da "Great Firewall of China", que realiza censuras no domínio cibernético. Os roteadores-cebolas têm um número de IP atrelado ao espaço fisico da China. Os IP's são relativamente estáveis pois se encontram listados no diretório padrão da rede TOR, de modo que qualquer usuário possa escolher os roteadores desta lista para construir o seu próprio conjunto de circuitos – como explicado anteriormente.

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).

A rede mundial de computadores tornou-se um importante canal de comunicação entre indivíduos no século XXI. Embora não tenha versado especificamente sobre o domínio cibernético, Strange (1988) criticou especialistas que afirmavam que o mundo encarava a "Revolução da Informação" sem, pelo menos, (1) apontar que alterações esta suposta revolução realizaria no contexto das relações humanas, (2) ou o modo como deslocaria poder, (3) ou mesmo como poderia realocar os esforços das sociedades humanas em novas metas. De fato, ela concordava que ao final da década de 1980 o mundo dava grandes saltos tecnológicos, em parte apoiados sobre três grandes rápidas mudanças: o desenvolvimento de sistemas computacionais bastante sofisticados que permitiam o acesso em massa devido ao baixo custo; a extensão destes sistemas, utilizando inclusive satélites que orbitam a terra; e a digitalização do idioma, aproximando diferentes grupos humanos antes separados por não falarem a mesma língua. No entanto, apesar dessas alterações tecnológicas estivessem acontecendo, sua crítica residia no fato de que a maioria dos especialistas, à sua época, parecia apenas explicar o que a tecnologia estava fazendo e como ela estava operando. Ou seja, não realizavam considerações políticas sobre o elemento do poder frente a todas estas mudanças.[142] Aqueles que se arriscavam a realizar considerações sobre possíveis deslocamentos do lócus de poder, em razão das revoluções tecnológicas vigentes, divergiam em dois grandes grupos: aqueles que acreditavam que a alteração do lócus estava ocorrendo e aqueles que discordavam, acreditando que o lócus permanecia inalterado. Contudo, ela própria não posicionou-se em nenhum destes grupos mas apontou a estrutura do conhecimento como alternativa, devendo ser pensada junto das demais.

É importante lembrar que as reflexões iniciais de Strange (1988) sobre o aspecto tecnológico ao final do século XX, em *States and Markets*, ela discorria a partir de uma visão da década de 1980. Quando ela publica a obra *The Retreat of the State: The Diffusion of Power in the World Economy*, em 1996, a Internet já havia sido comercializada – ou seja, tanto parte da sociedade humana começava adentrar o ambiente do domínio cibernético navegando na Web pela primeira vez, como surgiam as primeiras empresas que proviam o acesso à malha cibernética da rede mundial de computadores. Em 1996, a Internet não mais encontrava-se isolada da massa, quase restrita apenas aos centros acadêmicos e militares, utilizada por cientistas da computação e

142 Política no sentido que Strange (1996) utiliza, ou seja, não necessariamente atrelado aos altos escalões do governo e políticos.

entusiastas – como na ocasião da publicação de 1988. Na década de 1980 sim, a Internet era isolada da grande massa. Oito anos depois, Strange (1996) admite que as cinco principais mudanças[143] ocorridas no setor das telecomunicações, nas demandas do mercado e nas ações políticas resultaram no deslocamento da autoridade dos Estados para atores não-estatais. Antes, o Estado concentrava praticamente em si o poder de controlar o conhecimento e os meios através dos quais a informação circulava – por correios, telégrafos ou telefones; na década de 1990, um conjunto de ações possibilitou a abertura de novas opções de canais de comunicação para empresas privadas e governos estatais. (STRANGE, 1996, p.100).

Conforme explicado em seções anteriores neste capítulo, a Internet é uma dimensão híbrida composta por infraestrutura física (cabos, satélites, computadores-servidores, computadores-clientes, etc.) e abstração digital (tecnologia que permite que dados percorram a rede segundo instruções específicas, linguagens computacionais, composição de bytes que resultam em arquivos digitais, protocolos, domínio cibernético, etc.). As considerações de Strange (1996) sobre este novo canal de comunicação – produzido a partir de importantes alterações tecnológicas calcada pelos sistemas de informações baseados em computadores, satélites e cabos de fibra ótica – parecem indicar que ela tratava, particularmente, da infraestrutura física da rede mundial de computadores. Ou seja, aproximou-se do guarda-chuva temático das telecomunicações mas não adentrou o tema *cyber*. É no domínio cyber que a existência da rede anônima TOR, componente da Dark Web, torna-se relevante pois, apesar de utilizar a infraestrutura da rede mundial de computadores (física) para funcionar, ela aplica-se sobre a camada TCP/IP (abstrato) para compor seu canal de operação.

Embora não tenha versado sobre o aspecto cyber, podemos realizar algumas observações a partir dos próprios insumos providos por Strange quando discutiu a estrutura do conhecimento, o poder estrutural e a difusão de poder. De acordo com ela, e retomando mais uma vez o cerne de sua discussão, a estrutura do conhecimento compreende (1)

143 De acordo com Strange (1996) as cinco principais mudanças foram: (1) melhoria nos sistemas de transmissão de informação (surgimento de fibra ótica, por exemplo); (2) aumento de tamanho de comutadores digitais capazes de servirem uma única grande região ou mesmo país pequeno; (3) invenção de telefones e celulares que não desprezam o uso de fios impulsionaram o novo mercado; (4) uso de satélites que orbitam a Terra; (5) sistemas de transmissões mais eficientes para computadores e telefones que permitiram a digitalização da informação, reduzindo consideravelmente o tempo e o espaço entre indivíduos.

crenças (incluindo aqui as conclusões morais e os princípios que derivam da crença); (2) todo o conhecimento humano, percebido e compreendido como tal; e (3) os canais por meio dos quais crenças, ideias e conhecimento são transmitidos de forma a permitir a comunicação – inclusive, o ato de incluir alguns indivíduos e excluir outros. Partindo disto, podemos afirmar que a rede anônima de baixa latência TOR faz parte da estrutura do conhecimento pelas seguintes razões.

Primeiro, a rede TOR foi concebida a partir de conhecimentos técnicos sobre computação bastante específicos que resultaram na implementação da tecnologia do "roteamento cebola". Ora, para que esta rede pudesse ser formulada, ela precisou assentar-se, sobretudo, na rede mundial de computadores – a qual também derivou de um conjunto de conhecimentos técnicos bastante específicos. A Internet, afinal de contas, foi o resultado de diferentes forças que, primeiro descobriram métodos de aplicação do conhecimento até então inéditos – como o caso de Paul Baran (1964) e a tecnologia da comutação de pacotes; Tim Berners-Lee que desenvolveu protocolos que culminaram na WWW; Marc Andreessen que implementou gráficos e imagens aos navegadores; entre outros. Sendo assim, a Internet é o amálgama do progresso de constantes ideias e implementação de projetos e conhecimentos inovadores que surgem ao final do século XX. E a rede TOR?

Segundo, a rede TOR foi desenvolvida por membros da sociedade civil – Roger Dingledine e Nick Mathewson, ambos através da Free Haven Project – e um membro do governo norte-americano – Paul Syverson, membro do Laboratório Naval Norte-americano. O design tecnológico que encontra-se no cerne da rede anônima, e pela qual seu nome deriva, é o "roteamento cebola". Este design visa implementar o anonimato nas comunicações e também sobre a localização do usuário na malha da Internet (lembrando que a rede TOR utiliza a infraestrutura da rede mundial de computadores). Cabe lembrar, como discutido em seções anteriores, que esta técnica de design vinha sendo discutida desde o início da década de 1990 – o que evidencia o processo de acumulação do conhecimento. Seus criadores classificaram a rede desenvolvida por eles como sendo parte da terceira geração a utilizar esta técnica. Este ponto é relevante porque demonstra, na prática, o que foi apontado por Strange (1988) em relação ao conhecimento: faz parte da estrutura do conhecimento o que é dito como conhecido e percebido como compreendido. Portanto, o conhecimento acumulado que possibilitou a criação da rede anônima TOR, e sobre qual a mesma

baseia-se para operar, por definição, é parte da estrutura do conhecimento – visto que este conhecimento é percebido como entendido e, inclusive, compartilhado ao redor do mundo por meio de cursos de graduação e centros educacionais sobre informática: é a área da Ciência da Computação, Sistemas de Informação e Informática no geral. Se a estrutura do conhecimento compreende tudo que é acreditado e percebido como compreendido, tanto a Internet como a rede anônima TOR fazem parte da estrutura do conhecimento – tal como definido por Strange (1988).

Terceiro, além disso, a rede TOR tornou-se relevante canal de comunicação para compartilhamento de ideias, conhecimentos e crenças. Cabe lembrar que Surface Web e Dark Web – do qual a rede anônima de baixa latência TOR faz parte – são regiões distintas do ciberespaço atual. A rede TOR, apesar de utilizar a infraestrutura da Internet, é uma rede em si própria e acessível apenas através do software TOR, próprio para navegação da rede de mesmo nome. Ao contrário da Internet, não é uma rede aberta no sentido de que é acessível por qualquer navegador convencional, bastando apenas digitar o nome do domínio na barra de endereços. Gerenciada pelo Tor Project, a relevância da rede TOR é atribuída ao caráter anônimo e à privacidade que oferta aos usuários e às informações trocadas por meio da rede. E essa relevância tem sido crescente tendo em vista a vigilância digital perpetrada recentemente por Estados e empresas privadas na Surface Web. (LANDAU, 2013; NOCETTI, 2015; LYON, 2015; MURATA, ADAMS, PALMA, 2017).

Em especial, a rede TOR auxilia aqueles que, por alguma razão, encontram-se em risco quando utilizam a Surface Web. É o caso de dissidentes políticos, ativistas digitais, ativistas de Direitos Humanos, jornalistas, denunciantes, etc. (TOR PROJECT, 2018). Um destaque é a organização sem fins-lucrativos Repórteres sem Fronteiras, fundada em 1985 na França. Esta organização, de caráter consultivo na Organização das Nações Unidas para a Educação, Ciência e Cultura (UNESCO), no Conselho da Europa e membro da Organização Internacional da Francofonia (OIF), está presente em 130 países por meio de rede de correspondentes. Ela tem divulgado no meio jornalístico, por meio de manuais, informações sobre o funcionamento da rede TOR e o auxílio que oferece aos profissionais da área com relação à blindagem da comunicação e das informações trocadas – incentivando-os a utilizar como meio principal de comunicação. (REPÓTERES SEM FRONTEIRAS, 2016). Para os Repóteres sem Fronteiras a rede TOR é

importante ferramenta de proteção aos dissidentes e resistência à censura. (OVERLIER; SYVERSON, 2005). Cabe lembrar que esta organização é conhecida mundialmente por produzir *The Internet Censorship Ranking*, em que lista os Estados de acordo com o grau de censura imposta na rede. (WARF, 2011). Mas os Repórteres sem Fronteiras não são os únicos que utilizam a rede TOR como relevante canal de comunicação para a execução de suas atividades. Pelo menos dois grandes jornais de grande circulação, The New York Times e The Guardian, ofertaram canal de comunicação pela rede TOR para que denunciantes pudessem compartilhar informações com o corpo editorial de modo seguro. (SANDVIK, 2018; THE GUARDIAN, 2018).

Se a estrutura do conhecimento compreende os canais por meio dos quais as crenças, ideias e conhecimentos são comunicados – tal como definido por Strange (1980) – é razoável assumir que, de maneira geral, a Internet é o mais recente canal de comunicação em massa vigente.[144] Neste novo canal de comunicação, incluem-se os usuários (antigamente conhecidos como "internautas") com acesso à rede e excluem-se aqueles marginalizados à ela (seja por falta de computador, seja por falta de provedor com capacidade de conectar a máquina à rede mundial, ou qualquer outra alternativa que impossibilite a entrada do indivíduo na malha da Internet). Através da rede mundial de computadores, por meio da implementação de diferentes protocolos, outros canais de comunicação operam no domínio "cyber" – como é o caso da rede TOR. E assim como a Internet no sentido geral, a rede TOR também possibilita a inclusão de algumas pessoas e a exclusão de outras na sua rede. A Internet e a rede TOR fazem parte da estrutura do conhecimento, sendo ambas constituídas a partir de esforço colaborativo entre a sociedade civil e o Estado para o desenvolvimento e criação de conhecimento e ferramentas de relevância social.

3.5 REDE TOR E CYBERPOWER

Enquanto Susan Strange ateve-se ao tratamento do poder no plano real geográfico, Joseph Nye realizou considerações acerca do elemento poder no domínio cibernético indicando que este seria o "futuro do poder" – inclusive título de obra de 2011, *The Future of*

[144]Especialmente se comparado aos outros canais de comunicação expostos por Strange (1996): o sistema de telégrafos, correios e telefones [PPTs].

Power. Existem pelo menos quatro elementos de discussão na obra do Nye que são pertinentes a esta pesquisa e que discutiremos brevemente: a difusão de poder; a estrutura do conhecimento; definição de "cyberpower"; incidência dos resultados dentro e fora do plano cibernético.

Sob um primeiro olhar, leitores podem indagar sobre as semelhanças e diferenças quanto ao fenômeno da difusão de poder elaborados por Strange (1996) e Nye (2011). Enquanto a primeira discutia difusão de poder como desconcentração qualitativa do poder na figura do estado diluindo-se no tecido econômico-político internacional em direção a atores não-estatais com autoridade e poder suficiente para redefinir as opções dos demais, o segundo discutia a difusão de poder no domínio cibernético. Esta difusão de poder, segundo Nye (2011), era promovida pelo fato da redução dos custos de entrada de atores na região do ciberespaço. Dentro desta região cibernética, os atores utilizam de mecanismos e ferramentas próprias deste espaço para lograr atingir resultados desejados. Ambos tratam sobre domínios distintos, plano real e plano cibernético, porém concluem que a difusão de poder trata sobre o deslocamento de poder concentrado na figura estatal em direção a atores não-estatais. Diante da análise do banco de dados presente nesta pesquisa, podemos concluir que existe, de fato, o surgimento de atores não-estais no domínio cibernético que realizam operações de tal maneira que alcançam os objetivos desejados por si. Além disso, verificamos que estes atores podem ser diversos – desde pesquisadores e especialistas em segurança cibernética que agem de modo individual, até organizações preocupadas em manter o funcionamento de rede anônima criada por si própria e utilizada por diversos outros atores. A redução dos custos de entrada, como sugerido por Nye e refletido na dicotomia entre melhoria tecnológica e diminuição de preços, permite a presença destes indivíduos na rede digital baseada na microeletrônica. Estes atores diversos são protagonistas das mais distintas operações em curso na região do ciberespaço. Neste sentido, o Estado não é o único ator com autoridade, controle ou capacidade de alterar o status-quo – evidência da difusão de poder em curso. Para Nye, em um mundo cada vez mais baseado na informação, a difusão de poder e o surgimento de atores não-estatais torna-se uma ameaça potencialmente mais problemática do que a transição de poder entre ocidente e oriente, uma vez que a difusão de poder atesta a falta de controle do Estado.

Em relação estrutura do conhecimento, Nye não utiliza, explicitamente, o paradigma da EPI sugerido por Strange baseado em quatro estruturas primárias. Porém, torna-se claro que, em diversos momentos de sua obra, ele versa sobre a relevância de atores posicionados dentro da estrutura do conhecimento ou, até mesmo, sobre a estrutura em si. Para Nye, a informação ocupa poder crucial nesta nova era, afirmando que "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). Como se sabe, a informação/conhecimento é o elemento principal da estrutura do conhecimento – o que evidencia que, indiretamente, esta estrutura ocupa posição de destaque na nova dinâmica do poder, segundo perspectiva do autor.

Diferentemente de Strange, Nye cunhou definição para o poder que opera no domínio cibernético: "cyberpower". Este poder ganha contornos a medida que é definido por meio de um conjunto de recursos que relaciona-se aos sistemas de informação baseado na computação. Nye afirma que "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). Uma interpretação disto é que o poder cibernético está intimamente envolvido com conjunto de recursos relacionados a estrutura do conhecimento e a dimensão controle. Estrutura do conhecimento pelo elemento da criação, que acontece a partir do acúmulo de conhecimento sobre uma determinada matéria – neste caso, conhecimento baseado na computação. Controle e comunicação relacionam-se com a estrutura do conhecimento na medida que o controle dos canais de comunicação proporcionam posição de destaque àqueles em sua posse. E dimensão controle porque evidencia a difusão de poder em direção àquele de posse do controle sobre um objeto relevante para seus fins no domínio cibernético. Para Nye, "cyberpower is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyberdomain." (NYE, 2011, p.123). O poder cibernético pode ser interpretado como uma adaptação do poder relacional no domínio do ciberespaço. se compreendemos que obter os resultados desejados refere-se a alteração do status-quo (em que não havia alcance dos resultados desejados), há indícios de que o "cyberpower" definido por Nye opera, pelo menos, em duas dimensões: controle e resultados. Nye, entretanto, considera que a alteração do status-quo pode ter

consequências tanto dentro como fora do ciberespaço. Ele afirma que "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). Apesar de concordar que a alteração do status-quo possa incidir dentro do domínio do ciberespaço, nós buscamos tratar das consequências que incidissem sobre a realidade geográfica, para fins desta pesquisa.

3.6 CONCLUSÃO

O presente capítulo 2 desta dissertação buscou discursar acerca dos assuntos relacionados ao histórico e funcionamento da Internet, a classificação da Dark Web no contexto da WWW e as tecnologias específicas da rede anônima TOR. A partir disto, discutiu-se os chamados "serviços ocultos" da Dark Web, o papel político da criptografia e a popularidade da rede anônima TOR. Por fim, buscamos fundamentar a rede anônima TOR como parte relevante da estrutura do conhecimento no século XXI.

Inicialmente, nós buscamos fundamentar as razões pelas quais acreditamos que a rede anônima TOR insere-se como parte da estrutura do conhecimento – elemento conceitual definido por Strange (1988) ao final da década de 1980. Apesar de não ter versado, explicitamente, sobre a Internet, Strange (1996) destacou a relevância dos sistemas de informação, o uso de satélites e a tecnologia desenvolvida pela computação sobre as comunicações humanas. Nossa análise incidiu-se sobre uma região específica do ciberespaço que é produto de conhecimentos acumulados e reunidos, principalmente, por indivíduos da sociedade civil – embora, no caso da rede TOR, tivesse a presença de um membro do setor público na origem do desenvolvimento da rede.[145] Como último elemento apresentado, nós evidenciamos algumas considerações acerca da rede anônima TOR e o "cyberpower" definido por Nye (2011).

Acreditamos que o conteúdo abordado neste capítulo seja revelante e necessário para a análise de difusão de poder do capítulo seguinte. Sendo assim, no próximo capítulo, abordaremos os artigos jornalísticos por meio dos quais originou-se os atores não estatais que

[145] Especificamente membro do Laboratório Naval da Marinha dos EUA.

participaram de nossa análise. Nós apresentamos, por fim, os resultados da difusão de poder em três dimensões para grupos temáticos individualmente e comparados entre si. Além disso, iremos expor a difusão de poder de modo geral sobre o total de ocorrências.

4. CAPÍTULO 3: ANÁLISE DE DIFUSÃO DE PODER NA REDE TOR EM TRÊS DIMENSÕES

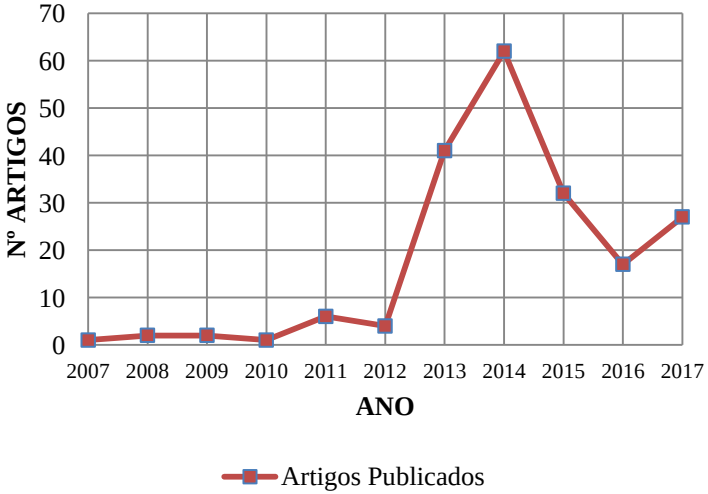
O terceiro capítulo desta dissertação tem como objetivo apresentar as análises de difusão de poder em três dimensões realizadas a partir de banco de dados composto por informações oriundas de aritgos jornalísticos. No banco de dados estão expostas as variáveis "autoridade", "controle" e "resultados" que surgem a partir da operacionalização das três dimensões de mesmo nome. De modo a fornecer contexto para as variáveis, nós também identificamos outras informações relevantes como a identificação dos pares e interessados (relativo a dimensão autoridade), o objeto considerado relevante para o alcance do resultado desejado pelo ator não-estatal no contexto do artigo (relativo a dimensão controle) e o efeito sobre a realidade (relativo a dimensão "resultados"). Além disto, o banco de dados é composto por outras informações relacionadas com a identificação dos artigos de jornal como autores, jornais, país-sede, título do artigo, etc.

A análise foi feita de acordo com a metodologia definida na Introdução desta dissertação e utiliza a operacionalização do fenômeno de difusão de poder – a partir da frequência de ocorrências de cada variável, o que nos permitiu gerar quadros estatísticos. Para fins desta dissertação, a partir das leituras dos artigos nós identificamos os atores não-estatais e os agrupamos de acordo com temas comuns à eles. A partir disso, nós apresentaremos os resultados da análise de difusão de poder em três dimensões autoridade, controle e resultados: para cada dimensão foram expostos os resultados da (a) análise individual de cada grupo temático, (b) análise comparada entre os grupos temáticos e (c) análise geral sobre o total de ocorrências. Os gráficos, tabelas e quadros que surgiram a partir da interpretação dos dados, juntamente com o banco de dados com 139 ocorrências, encontram-se no apêndice da dissertação.

4.1 FREQUÊNCIA JORNALÍSTICA SOBRE A REDE TOR

A fim de compreender a publicidade dada por estes jornais sobre o tema da rede anônima, nós averiguamos o número de publicação de artigos por ano e, assim, obtivemos o seguinte gráfico.

GRÁFICO 1 - NÚMERO DE ARTIGOS RELACIONADOS A "TOR NETWORK" PUBLICADO POR ANO (2007-2017)



Os 195 artigos estavam distribuídos no período de uma década, como exposto acima. A partir deste gráfico, podemos fazer algumas observações acerca da média de artigos publicados anterior ao ano de 2013, o crescimento do número de publicações em 2013- 2014 e 2017 e a mudança de patamar após o ano de 2014.

Inicialmente, entre os anos de 2007 a 2012, observamos poucos artigos publicados pelos jornais supracitados – 13 artigos no total. Esta média altera-se nos anos seguintes. Em 2013, o número de artigos publicados supera a marca de 40. Três atores assuntos majoritariamente responsáveis por este aumento: (1) a organização ativista Tor Project, responsável pela manutenção, melhoria e operacionalização da rede anônima, foi citada ao longo das notícias que evidenciavam a própria rede TOR ou o tema da Dark Web; (2) o mercado anônimo online Silk Road, que teve seu principal responsável, Ross Ulbricht, encarcerado pelas autoridades norte-americanas em outubro de 2013; (3) e as revelações de Edward Snowden, que expuseram o esquema de vigilância global perpetrado pelo governo dos EUA e demais aliados.[146]

[146] Ver "Apêndice 5 – Artigos Publicados em 2013".

Em 2014, o número de publicações alcança o patamar de 60 artigos – 50% a mais que o ano anterior. Além dos assuntos mencionados anteriormente, outros três também contribuíram para o aumento: (a) a ascensão do mercado online Silk Road 2.0, que buscou a continuidade da versão anterior fechada em 2013 por autoridades policiais dos EUA; (b) a operação de redes transnacionais de pornografia infantil pela rede anônima; (c) e a exposição do tema sobre privacidade e anonimato na Internet.[147]

Enquanto no período de 2013 e 2014 houve crescimento do número de artigos publicados relativos a rede anônima TOR, nos anos seguintes ocorre decrescimento do número destas publicações. Apenas em 2017 há leve crescimento deste número. É relevante notar que após o ano de 2014, as publicações relacionadas a rede anônima TOR mudam de patamar se comparados ao momento anterior ao ano de 2013: antes não alcançavam 10 publicações ao ano, e depois não publicavam menos que 15 artigos de notícia. Esta mudança de patamar reflete o interesse das abordagens jornalística sobre, principalmente, os chamados "mercados anônimos" da Dark Web. Estes mercados são conhecidos especialmente por comercializar drogas, entorpecentes e demais substâncias ilícitas. Em 2017, por exemplo, o mercado Alphabay domina as publicações jornalísticas que envolvem a rede anônima TOR. Mas a mudança de patamar também reflete a cobertura jornalística dada às prisões de administradores e responsáveis por redes de pornografia infantil pelas autoridades policiais de diversos governos.[148]

Neste período de dez anos, os jornais britânicos The Guardian e Mail Online e o jornal norte-americano The Washington Post foram aqueles que mais produziram artigos de notícias relacionados à rede anônima TOR. Os jornais orientais, Tribune Newspaper, People's Daily Online e Xhinua News Agency, foram aqueles que menos deram publicidade ao tema.

[147] Ver "Apêndice 6 – Artigos Publicados em 2014".
[148] Ver "Apêndice 7 – Artigos Publicados em 2017".

TABELA 4 - NÚMERO DE ARTIGOS RELACIONADOS A "TOR NETWORK" PUBLICADOS POR CADA JORNAL(2007-2017)

País	Jornais	N
Inglaterra	The Guardian	64
Inglateerra	Mail Online*	53
EUA	Washington Post	31
Inglaterra	Telegraph Media Group	17
EUA	Advance Digital**	17
EUA	The NY Times	11
India	Tribune Newspapers	1
China	People's Daily Online	1
EUA	Hearst Newspapers	0
China	Xinhua News Agency	-
Total		**195**

Fonte: Autora.

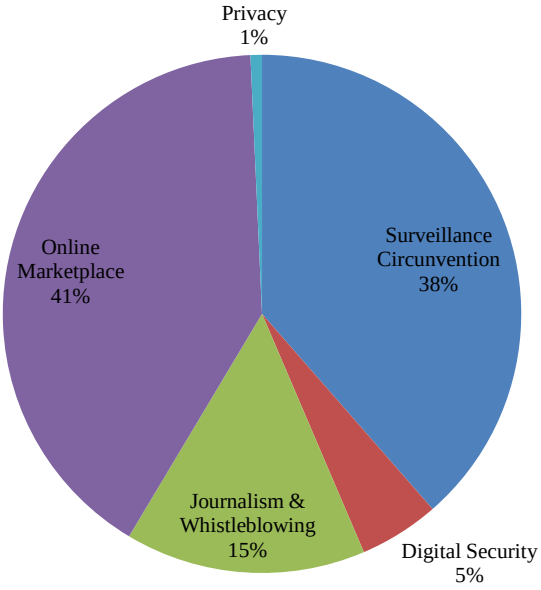
4.1.3 Atores e Grupos Temáticos Oriundos dos Artigos Jornalísticos

A partir da elaboração do banco de dados, identificamos 26 atores oriundos de 139 ocorrências (estas provenientes de 125 artigos de jornais). Estes atores foram alocados dentro de 5 categorias formuladas por nós que correspondem a grupos temáticos distintos. Esta classificação foi elaborada a partir da leitura dos 125 artigos de jornal.

O primeiro grupo temático, **Digital Security**, compreende os atores relacionados à segurança da informação e da rede: Dan Egerstad; Freedom Hosting; Iranian Cyber Army; Onion Ransomware; Ransomware; SimpleLocker Android Malware; Carnegie Mellon University. O segundo grupo temático, **Surveillance Circunvention**, abrange atores que, de algum modo, "driblam" a vigilância digital perpetrada, principalmente, por atores estatais: Tor Project e Facebook. O terceiro grupo, **Online Marketplace**, é composto por mercados onlines anônimos que operam na rede TOR: Silk Road; Silk Road 2.0; Silk Road 3.0; Alphabay; Farmer's Market; Evolution e Sheep Marketplace. O quarto grupo temático, **Journalism & Whistleblowing**,

compreende atores engajados com denúncias de informações sigilosas ou envolvidos com a profissão do jornalismo: Edward Snowden; WikiLeaks; SecureDrop System; Strongbox; ProPublica; Harold T. Martin; Chelsea Manning e X-Net Group. E, finalmente, o grupo **Privacy** envolve atores que, de alguma forma, estão relacionados com a exposição de dados e a privacidade de indivíduos: Doxbin.

GRÁFICO 2 - (%) OCORRÊNCIAS POR GRUPO TEMÁTICO (2007-2017)



O grupo que apareceu com mais frequência nos artigos de jornal, em porcentagem, foi o grupo Online Marketplace, com 41% das ocorrências sobre atores envolvidos com a comercialização de produtos, serviços e bens ilícitos na rede anônima TOR. Em seguida, surge o grupo Surveillance Circunvention, com 38% das ocorrências relatando ações dos atores que compõem este grupo. O destaque é dado ao ator

Tor Project, responsável pela manutenção da rede anônima TOR, melhorias e ativismo digital. Em terceiro lugar, o grupo Journalism & Whistleblowing, com 15% das ocorrências expondo ações de atores que lidam com o jornalismo ou estão, de alguma forma, envolvidos com denúncias. Finalmente, ogrupo Digital Security, com 5%, e em último lugar o grupo Privacy, com 1% das ocorrências.

O primeiro grupo temático, Digital Security, dispõe de seis atores relacionados à segurança técnica da informação e da rede no geral.

O pesquisador de segurança, **Dan Egerstad**, de 21 anos, foi responsável por encontrar falhas de segurança nas comunicações de diversas embaixadas como Rússia e Índia. De acordo com Kirk (2007), Egerstad conseguiu realizar o download de arquivos confidenciais. As embaixadas utilizavam a rede TOR com o objetivo de proteger suas comunicações mas, como apontado por Egerstad, elas falharam em proteger os nódulos de entrada e saída da rede TOR com criptografia. Cabe lembrar que os nódulos centrais dos túneis criados pelo TOR são automaticamente criptografados – mas não aqueles de entrada e saída, que necessitam que o usuário manualmente proteja-o com camada criptográfica. (KIRK, 2007). O conhecimento do jovem pesquisador em segurança possibilitou a descoberta de relevantes falhas na comunicação entre as embaixadas, bem como remediá-las.

O **Iranian Cyber Army** é um grupo que realiza atividades no domínio cibernético e que trabalha juntamente ao governo iraniano. (CUBRILOVIC, 2009). De acordo com a notícia escrita por Cubrilovic (2009), o grupo desferiu ataques aos servidores responsáveis por hospedar os registros de DNS do Twitter. Com acesso à conta do Twitter, o Iranian Cyber Army alterou os registros de DNS do endereço "twitter.com" de modo que, em vez de redirecionar para o servidor padrão, indicassem um endereço de IP específico da rede anônima TOR. Este ataque coincidiu com a escalada de hostilidade diplomática entre o Irã e EUA, bem como a incursão de tropas iranianas próximo às fronteiras de disputa de petróleo. (CUBRILOVIC, 2009).

Os próximos três atores – **Onion Ransomware, Simple Locker Android Malware** e **Ransomware** – são softwares, desenvolvidos por um indivíduo ou conjunto de indivíduos, que têm como objetivo o "sequestro" de determinados arquivos ou funcionalidades de dispositivos do usuário. Os arquivos e funcionalidades são retornados apenas mediante o pagamento quantias monetárias. Este tipo de software é conhecido pela literatura como "ransomware". (GAZET, 2014;

SCAIFE et al, 2016). Destes três ransomwares mencionados acima, o primeiro deles, "Simplelocker Android Malware" foi reportado em junho de 2014 por Tom Brewster. De acordo com o jornalista, este ransomware atacou dispositivos que utilizavam o sistema operacional "Android" realizando uma varredura na memória dos aparelhos para criptografar determinados arquivos e, assim, demandar pagamento por parte do usuário para a recuperação dos dados. Os arquivos sequestrados por este ransomware eram enviados para servidores dentro da rede TOR. (BREWSTER, 2014). O segundo destes ransomwares, "Onion Ransomware", foi reportado em julho de 2014 por Alex Hern. Segundo o jornalista, este ransomware era responsável por sequestrar arquivos dos dispositivos do usuário, utilizando a rede TOR para manter oculta a sua natureza técnica e atividades. Uma vez que o dispositivo era infectado com o "Onion"[149], o mesmo dispunha de uma tela com tempo de 72 horas realizando a contagem regressiva deste tempo. Caso o pagamento não fosse realizado neste período, os arquivos eram descartados. (HERN, 2014). O terceiro ransomware, descrito por Charles Arthur em 2017 apenas como "Ransomware", atacou diversos hospitais no Reino Unido. Como de praxe, demandava o pagamento de quantias de dinheiro pela recuperação dos dados e arquivos. Mas o pagamento, neste caso, deveria ser realizado por meio da moeda digital critptográfica "BitCoin" à uma página hospedada na rede TOR. (ARTHUR, 2017).

O último ator da categoria em questão é o servidor **Freedom Hosting**. Este servidor, em 2013, foi considerado o maior da rede anônima TOR – e, geralmente, associado com conteúdo ilícito. (PETERSON, 2013). Em 2013, ele foi infectado por um "malware" que acredita-se ter sido implantado pelo Federal Bureau of Investigation (FBI) com o objetivo de retirá-lo de funcionamento. Para isso, o malware utilizou-se de uma brecha de segurança em versões antigas do navegador convencional "Firefox"[150] para implantar-se no servidor Freedom Hosting e utilizar código próprio desenvolvido para identificação dos usuários que acessassem o servidor. Destaca-se aqui que a brecha foi encontrada no navegador Firefox, ou seja, não houve brecha de segurança na rede TOR. (PETERSON, 2013).

149Não confundir com The Onion Router (TOR) ou o design técnico conhecido como "Onion Routing". Neste caso, "Onion" é apenas o nome deste ransomware específico.

150A empresa "Firefox" optou por inserir ao seu navegador recursos do próprio navegador Tor para aumentar a privacidade dos seus usuários.

A universidade norte-americana **Carnegie Mellon University** é uma instituição privada do setor da educação, sediada na Pensilvânia, EUA. Segundo Alex Hern (2016), o departamento de defesa dos EUA financiaram pesquisas da universidade Carnegie Mellon com o objetivo de descobrir táticas que pudessem remover o "anonimato" dos usuários da rede TOR. A organização Tor Project identificou, no início de maio de 2014, que alguns nódulos da rede anônima aparentavam direcionar seus esforços na identificação dos demais nódulos e, por esta razão, foram removidos da rede em junho do mesmo ano. No mês seguinte, em julho de 2014, pesquisadores da Carnegie Mellon cancelaram a apresentação pública de um artigo cujo conteúdo buscava revelar táticas de identificação de IP's dos usuários da rede TOR. Hern (2016) aponta que documentos liberados pela corte do caso Silk Road confirmaram o envolvimento da universidade Carnegie Mellon na identificação dos nódulos da rede anônima e as informações recolhidas foram acessadas pelo FBI. (HERN, 2016).

O segundo grupo temático, "Surveillance Circunvention", destaca dois atores que oferecem meios para driblar a vigilância digital: o Tor Project, através da rede anônima de mesmo nome, e o Facebook, que é a primeira plataforma de mídia social a oferecer acesso por meio da rede de baixa latência.

A organização sem fins-lucrativos **Tor Project**, responsável por gerenciar a rede anônima TOR, está intimamente relacionada com a oferta de métodos que driblem a vigilância digital especialmente perpetrado por alguns países sob a forma de censura. De acordo com Vitaliev (2008), Bradbury (2008) e Anderson (2009), o Tor Project ofereceu alternativa de acesso à Internet aos usuários residentes na China e no Irã, países reconhecidamente autoritários em manter rígida censura sobre diversos conteúdos dispostos na Internet. A China é conhecida por utilizar um sistema de "firewall" para filtrar conteúdo e restringir o acesso de cidadãos e residentes chineses que ficou conhecido na literatura como "The Great Firewall of China". (CLAYTON, MURDOCH, WATSON, 2006; ANDERSON, 2012; ENSAFI et al, 2015). O governo do Irã, por sua vez, ficou conhecido por controlar "gateways" de saída – especialmente em momentos pré-eleições e durante agitações populares. (ANDERSON, 2009). O Tor Project é conhecido por fornecer "Tor Bridges"[151] à usuários que tenham a

151Mais sobre "Tor Bridges" foi discutido no capítulo 2.

intenção de driblar a censura e utilizar livremente o acesso à Internet por meio da rede TOR.

A plataforma **Facebook** começou como uma rede privada para estudantes da universidade de Harvard lançada em fevereiro de 2004 na Surface Web. Atualmente o Facebook é uma empresa privada sediada na Califónia e amplamente utilizada na Surface Web por usuários de diversos países. Em outubro de 2014, de acordo com Fox-Brewster (2014), o serviço de mídia social abriu endereço na rede TOR, oferecendo canal de acesso aos usuários que navegam pela rede anônima. O objetivo não é prover anonimato aos usuários que acessam o serviço pelo TOR – uma vez que estes acessam perfis identitários quando entram no serviço Facebook – mas sim de driblar a censura em regiões autoritárias e vigilâncias digitais realizadas por entes locais, além de oferecer camadas adicionais de proteção à conexão. (MOYER, 2014).

O terceiro grupo temático, "Online Marketplace", abrange sete mercados online que operam, ou operavam, na rede TOR e eram conhecidos popularmente entre os usuários como "mercados negros da rede" e divulgados em sites de notícias da Surface Web. Martin (2013) propõe o tratamento dos mercados anônimos online como parte de um novo conceito de cibercrime – "cryptomarket" – cuja intenção é destacar esta área emergente de crimes específicos. De acordo com o autor, *"*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). Os tipos de bens e serviços comercializados nas "cryptomarkets", especialmente o comércio ilegal de drogas, justificam o tratamento destes mercados como parte do conceito de crimes cibernéticos. De qualquer modo, a literatura do assunto ressalta a modernidade do fenômeno dos mercados anônimos

152" Alguns mercados online criptografados são considerados pela literature. Martin (2013), por exemplo, define o que é um mercado deste tipo consideado ideal: "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) observam as "cryptomarkets" como um "submundo digital" ("digital demimonde"), ou seja, um mundo isolado e marginalizado do cotidiano que opera nas "fringes of the publically accessible Internet (through
Tor) and social mores." (MADDOX et al, 2015, p.111-112).

online e o desafio que apresentam às forças policiais.[153] (BARRATT, LENTON, ALLEN, 2012; CHRISTIN, 2013; MARTIN, 2013; RON, SHAMIR, 2014; VAN HOUT, BINGHAM, 2014).

O primeiro destes mercados, e o mais conhecido e amplamente discutido pela literatura, é o mercado online **Silk Road** – lançado em fevereiro de 2011, como um serviço oculto da rede de baixa latência TOR, e fechado pelo FBI em 2 de outubro de 2013. (CHRISTIN, 2013; BIRYUKOV, PUSTOGAROV, WEINMANN, 2014; BRADBURY, 2014; RON, SHAMIR, 2014; VAN HOUT; BINGHAM, 2014; MADDOX et al, 2015). Seu nome faz alusão à antiga Rota da Seda, rede de comércio que ligava os continentes europeu, africano e asiático.[154] (PHELPS; WATTS, 2014). Ele ficou conhecido como sendo um mercado criptografado especializado no comércio ilegal de drogas. (MADDOX et al, 2015). De acordo com Christin (2013, p.8), as 4 categorias[155] mais populares do mercado são referentes às drogas, enquanto que 6 categorias do "top 10", e 16 categorias do "top 20", são relativas aos narcóticos e entorpecentes. Desse modo, apesar de não comercializar exclusivamente drogas, o mercado, majoritariamente, lidou com o comércio de entorpecentes – ofertados por diversos vendedores diferentes.[156] As drogas eram comercializadas, sobretudo, em pequenas quantidades de modo a atender os interesses dos usuários.[157] (MARTIN, 2013). Por estas razões, além de apresentar uma

153 O caráter anônimo é conferido mediante o uso, também, de moeda digital de natureza criptográfica para realizar pagamentos – como, por exemplo, a moeda Bitcoin. (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).

155 Christin (2013) realizou um estudo que acompanhou o mercado anônimo Silk Road entre o período de 3 de fevereiro de 2012 até 24 de julho de 2012 e, neste período, pôde constatar o volume de 24.385 itens (únicos, ou seja, não repetidos) sendo comercializados. O mercado distinguia por volta de 220 categorias diferentes de produtos que envolviam desde produtos digitais até narcóticos e medicamentos com requisição de receita médica.

156 Corroboram com esta visão Biryukov, Pustogarov e 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). Em relação ao impacto econômico Martin (2013, p.353) afirma que, enquanto o comércio

interface amigável de compras online, o mercado Silk Road ficou conhecido como o "E-Bay das Drogas". (VAN HOUT; BINGHAM, 2014; MARTIN, 2013; PHELPS, WATTS, 2014; MASONI, GUELFI, GENSINI, 2016).

A administração do Silk Road era feita por uma pessoa, cuja identidade permaneceu desconhecida durante sua atividade, que se intitulava "Dread Pirate Roberts" (DPR) e que controlava todos os aspectos de operacionalização.[158] (RON; SHAMIR, 2014). Quando o mercado foi fechado pelas forças policiais, sua identidade foi revelada: tratava-se do cidadão norte-americado Ross Ulbricht – que à época da captura tinha 29 anos de idade. (BRADBURY, 2014). De acordo com o documentário "Deep Web", 2015, dirigido por Alex Winter, em que relata a jornada de Ross Ulbricht, durante a criação do mercado negro, o jovem norte-americano deixou pistas sobre sua identidade ainda na Surface Web – como seu endereço de e-mail pessoal em fóruns de comunicação online. O fechamento do mercado foi considerado o primeiro ato significativo das forças policiais em interromper o ambiente de um mercado online criptográfico e aconteceu em outubro de 2013. (MADDOX et al, 2015, p.122). No entanto, logo após este fato, surgiram outros mercados criptográficos online dedicados às transações de caráter anônimo como o Silk Road 2.0, "Atlantis" e o "Agora".[159] (BERGHEL, 2017).

O fechamento do mercado negro online Silk Road não indicou o fim dos mercados online que operam serviços na rede TOR. (POWER, 2013). Na verdade, no mês seguinte ao fechamento do Silk Road pelo FBI e DEA, surgiu a segunda versão do mercado negro: **Silk Road 2.0** – cuja intenção era continuar a marca Silk Road sob nova liderança. (DEMANT; MUNKSGAARD; HOUBORG, 2016). De acordo com

---

norte-americano gerou, aproximadamente, 300 bilhões de dólares norte-americanos no ano de 2005, o Silk Road correspondeu à um comércio menor de, aproximadamente, 23 milhões de dólares norte-americanos no mesmo ano.

158 Phelps e Watts (2014, p.2) apontam que a identidade por trás do pseudônimo "Dread Pirate Roberts" não pode ser confirmada como sendo de uma única pessoa. Provavelmente, a dificuldade de confirmar a exclusividade do pseudônimo apenas à Ulbricht aconteça em razão da origem do próprio pseudônimo – no filme "Princess Bride", 1987, dirigido por Rob Reiner, "Dread Pirate Roberts" era o pseudônimo utilizado por várias personagens que executavam o mesmo papel ao longo de gerações.

159 Sobre isso, Lacson e Jones (2016) argumentam que o fim do popular mercado não significa a interrupção, ou o fim, do ambiente da Dark Web – uma vez que seu final pode ser interpretado como parte de uma narrativa contínua, e do desenvolvimento, dos mercados negros da Dark Web. Christin (2013, p.2) ressalta ainda a existência de outros mercados anônimos online como o "Black Market Reloaded", "The Armory" e o "The General Store".

Demant, Munksgaard e Houborg (2016), no período entre novembro de 2014 a abril de 2015, o mercado Silk Road 2.0 comercializou cerca de 66 milhões de dólares norte-americanos – Cannabis foi o produto mais vendido. O mercado era gerenciado por Blake Benthall, norte-americano de 26 anos residente da Califórnia, engenheiro de software no Vale do Silício – mais precisamente, ele trabalhava para a empresa "SpaceX" do empresário Elon Musk. (ASSOCIATED PRESS; PRIGG, 2014). Um ano após sua abertura, Blake Benthall foi preso por forças policiais norte-americanas durante operação internacional orquestrada por diferentes países, "Operation Onymous", com envolvimento da Europol e cujo objetivo era deter crimes relacionados ao narcotráfico e operados no domínio cibernético. Agentes policiais infiltraram-se no mercado negro, ganhando confiança e recebendo valores para administrar determinados pontos do Silk Road 2.0 – o que lhes garantiu acesso à informações privilegiadas. (FOX-BREWSTER, 2014; RUSHE, 2014).

Novamente, em novembro de 2014, na sequência do fechamento do mercado online Silk Road 2.0, surgiu na rede anônima TOR o mercado **Silk Road 3.0 Reloaded** – seguindo a continuação da marca Silk Road. (ASSOCIATED PRESS, 2014).

Outro mercado negro influente na rede TOR foi o **Sheep Marketplace**, que surgiu logo após o fechamento do primeiro Silk Road e foi "invadido" por vendedores e consumidores que buscavam um mercado alternativo para continuar suas transações comerciais. (GARDNER, 2013). Este mercado negro também comercializava diferentes produtos, dentre os quais drogas e armas eram os principais. Assim como o Silk Road, o mercado Sheep Marketplace conduzia as transações financeiras na moeda BitCoin, e também adotou o mecanismo de pagamento conhecido como "escrow"[160]. No entanto, pouco tempo depois de receber grande volume de usuários órfãos do

160Este sistema era característico do mercado Silk Road. Seu objetivo era prover algum grau de confiança nas transações financeira entre compradores e vendedores – já que ambos são anônimos no mercado negro. De acordo com Bradbury (2014), seu funcionamento era da seguinte forma: "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 e Watts (2014) complementam, afirmando que o sistema "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)

Silk Road, o Sheep Marketplace fechou as portas, levando consigo grandes quantidades de BitCoin de usuários cadastrados no mercado – o que levantou suspeitas de que, na verdade, fosse um esquema para sequestrar moedas BitCoins. (GARDNER, 2013).

O mercado negro **Farmer's Market** também operava na rede anônima TOR, porém, diferente dos demais, aceitava outras formas de pagamento que não fossem na moeda digital criptográfica BitCoin – como dinheiro e transações via Paypal e Western Union. (ASSOCIATED PRESS, 2012). Este mercado foi gerido por oito homens de diferentes nacionalidades que, juntos, promoviam o encontro entre fornecedores de drogas, como LSD, Ecstasy e Ketamine e consumidores em potencial por meio do mercado online. Forças policiais dos EUA, Colombia, Países Baixos e Escócia atuaram juntos na operação "Adam Bomb" cujo objetivo era prender os oito indivíduos – e realizaram esta atividade com sucesso. (ASSOCIATED PRESS, 2012). Nesta mesma linha também agiu o mercado **Evolution**, que também viu o número de usuários crescerem após a captura de Ross Ulbricht, o administrador do Silk Road mais conhecido sob a alcunha de "Dread Pirate Roberts". Este mercado, que também servia de ponto de encontro entre vendedores e compradores de mercadorias ilícitas, igualmente desapareceu da rede anônima TOR, mas não sem antes levar consigo grandes somas de moedas BitCoins presos no sistema "escrow" do mercado. (FARRELL, 2015). Este "desaparecimento" da rede levou o pesquisador Henry Farrell (2015) concluir que, para erradicar os mercados negros da Dark Web, basta que a força policial cause impacto com a apreensão de um número suficiente administradores por trás dos mercados para que os demais ponderem sobre o futuro do mercado a longo prazo e desistam de operar criminalmente na rede.

Finalmente, o último mercado negro online da rede anônima TOR a aparecer nos artigos de jornais que compõem o banco de dados desta pesquisa é o mercado **AlphaBay**. À semelhança dos demais, este mercado também possibilitava a transação comercial de diversas substâncias ilícitas e serviços diversos. Além disso, foi um dos mercados com maior quantidade de tempo ativo em operação – de dezembro de 2014 a julho de 2017 . (TZANETAKIS, 2018). Estima-se que a categoria "Stimulants", como a cocaína, representava 20,98% das substâncias comercializadas no mercado – seguida da categoria "Cannabis & Hashish", com 18,47%, "Opioids", 12,69% e "Ecstacy" quarto, com 11,69%. (TZANETAKIS, 2018). Enquanto ativo, o mercado Alphabay foi considerado um dos maiores mercados de drogas

online, em número de produtos e usuários da página – providenciando um ambiente altamente competitivo. (PAQUET-CLOUSTON; HETU; MORSELLI, 2018). No mercado Alphabay, os vendedores deveriam pagar uma taxa de registro que custava em torno de 200 dólares estadunidenses – valor considerado baixo para entrada no mercado digital. (Ibid., p.95). Em julho de 2017, o AlphaBay foi fechado por forças policiais coordenadas por diferentes agências em diversos países. (TZANETAKIS, 2018).

O quarto grupo temático desta pesquisa, "Journalism & Whistleblowing", abrange oito atores que de algum modo estão relacionados com as atividades do jornalismo ou denúncias de esquemas ou segredos corporativos e/ou governamentais. Alguns deles são bastante conhecidos do público geral.

A organização sem fins-lucrativos **WikiLeaks** ganhou notoriedade, em 2010, após a divulgação de informações confidenciais de embaixadas norte-americanas, articulando-se com outros cinco jornais de grande circulação mundial – The New York Times, The Guardian, Der Spiegel, Le Monde e El País. Além disso, também ficou conhecido por expor um vídeo (conhecido como "Collateral Muder"), referente à Guerra do Iraque, de um helicóptero das forças armadas norte-americanas atacando deliberadamente civis iraquianos e, dentre eles, um fotógrafo da Reuters e seu motorista. (BENKLER, 2011; CURRAN, GIBSON, 2012). As ações do grupo WikiLeaks levaram estudiosos a repensar o cenário da diplomacia e do segredo após as revelações dos documentos. (HOOD, 2011; PAGE, SPENCE, 2011; BENKLER, 2011). O ex-porta-voz principal da organização, Julian Assange, atualmente encontra-se asilado na embaixada do Equador em Londres, Inglaterra. O website do grupo WikiLeaks na Surface Web fornece detalhes sobre o software TOR e explica para os usuários interessados os procedimentos necessários para instalar o programa na sua máquina de acesso à rede. (WIKILEAKS, 2016).

Chelsea Manning, previamente conhecida como Bradley Manning, serviu ao exército norte-americano durante a Guerra do Iraque como Analista de Inteligência, sendo responsável pelo vazamento de documentos secretos à organização WikiLeaks durante alguns meses e sua principal fonte. (ROTHE, 2013; MERCK, 2015). Manning posteriormente foi presa pelas autoridades norte-americanas – acusada de violar o Ato de Espionagem ("Espionage Act") e outros crimes contra os EUA – e sentenciada a 35 anos de prisão no dia 21 de agosto de 2013. (HACKL; BECKER; TODD, 2016). Ela recebeu o perdão presidencial

pelas mãos do 44º presidente norte-americano, Barack Obama , e libertada em maio de 2017. (PILKINGTON, 2017).

Edward Snowden, ex-empregado da empresa Booz Allen Hamilton, que mantinha serviços contratuais com o governo norte-americano, foi responsável por providenciar ao jornal britânico The Guardian documentos relacionados ao programa PRISM – cujo objetivo era a coleta de dados pessoais de milhões de indivíduos por meio de espionagem digital em massa operada sobre as comunicações via Internet. (LANDAU, 2013). O conjunto de documentos vazados por Edward Snowden ficou conhecido na literatura como "The Snowden Files". (CHADWICK; COLLISTER, 2014). O programa PRISM foi responsável por colecionar metadados das comunicações domésticas dos EUA, armazenando-os em provedores de serviços na "nuvem". (LANDAU, 2013). A agência britânica Government Communications Headquarters (GCHQ), equivalente a NSA para os EUA, permitiu a vigilância do órgão norte-americano sobre os cidadãos britânicos. (CHADWICK; COLLISTER, 2014). Após as relevações em 2013, Snowden recebe asilo por parte do governo russo e passa a residir no país. (MURATA; ADAMS; PALMA, 2017). Desde então, tem advogado a favor da privacidade e apoiado a organização Tor Project e a rede mantida por ela. (LEE, 2015) A rede anônima é, inclusive, alvo de ataques por parte da NSA e GCHQ – porém, sem sucesso. (BALL; SCHNEIER; GREENWALD, 2013).

Os jornais The Guardian e The New Yorker ambos apresentaram canais seguros, via rede anônima TOR, para que denúncias aos editoriais jornalísticos pudessem ser realizadas pelo público utilizando a Internet. Em 2013, o jornal The New Yorker lançou o serviço de compartilhamento de informações anônimas **Strongbox**, que funciona via TOR, e permite a comunicação blindada entre jornalistas e fontes. (PILKINGTON, 2013). De modo semelhante, o jornal The Guardian lançou em 2014, a plataforma de compartilhamento de informações em modo anônimo **SecureDrop System**, para que denunciantes pudessem submeter documentos confidenciais a jornalistas da instituição. (BALL, 2014).

O **X-Net Group** é um grupo ciberativista composto por mais de 200 voluntários que atua na Espanha aos moldes do WikiLeaks porém envolvidos na política do país e nas cortes de justiça. O grupo criou um canal de comunicação, via rede anônima TOR, para que indivíduos pudessem compartilhar documentos sigilosos e auxiliar na luta contra a corrupção. Apenas os voluntários registrados como "jornalistas" têm

acesso ao documento, por razões legais. Em outubro de 2014, o grupo foi responsável por denunciar esquemas de corrupção envolvendo oficiais de alto escalão do banco Bankia – banco espanhol fundado em 2010 durante o processo de reestruturação financeira da Espanha. (ASSOCIATED PRESS, 2014).

Três anos após as relevações de Snowden, **Harold T. Martin III**, ex-tenente da Marinha norte-americana, foi preso pelas autoridades do governo dos EUA sob acusações de espionagem e roubo de documentos sigilosos. Assim como Snowden, Harold Martin também trabalhava para a empresa Booz Allen, que mantinha serviços contratuais com a NSA. As autoridades descobriram grandes quantidades de documentos secretos do governo em sua residência, cujo conteúdo se tratava de arquivos do período entre 1996-2016. O ex-agente, treinado em segurança da computação, doutorando em "Information Security Management", Martin mantinha comunicações na língua russa e fazia uso de tecnologias criptográficas que permitiam o anonimato online. Em especial, o sistema operacional "Tails" que redireciona o tráfego de dados pela rede anônima TOR. (ASSOCIATED PRESS, 2016).

A organização sem fins lucrativos **ProPublica** é considerada a maior sala de redação independente de cunho investigativo no mundo, sediada em Nova York e ganhadora de um prêmio Pulitzer. Foi criada pela fundação de caridade "The Sandler Family Supporting Foundation", que doa cerca de 10 milhões de dólares anuais para a orgaização com o objetivo de fortalecer a democracia. (BROWNE, 2016). O jornalismo investigativo da ProPublica lançou plataforma de notícias na Dark Web em 2016, pela rede anônima TOR – cujo objetivo é proteger as comunicações dos usuários e dos servidores que armazenam as informações. Desde 2016, usuários de países que censuram a web, como a China, podem visitar a plataforma da ProPublica na rede TOR para acompanhar notícias sem temer a censura e o rastreio de dados e atividades. Além disso, usuários também podem compartilhar documentos e informações secretas através do serviço de denúncias do ProPublica na rede anônima. (JACKSON, 2016).

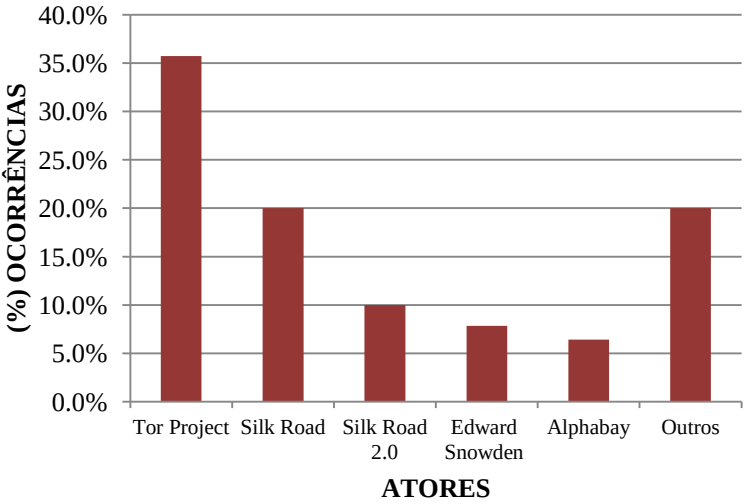
A cateogoria "Privacy" é composta pelo ator Doxbin, uma das páginas da rede anônima TOR que busca divulgar dados pessoais e informações privadas de indivíduos na rede.

A página da rede anônima TOR, **Doxbin**, foi fechada em 2014 por autoridades policiais conjuntas durante a operação Onymous. (FOX-BREWSTER, 2014). A página Doxbin praticava o que ficou conhecido

na literatura como “doxing” – o roubo de dados pessoais com o objetivo de maliciosamente denegrir ou desacreditar indivíduos. (LIBICKI, 2017). A prática de doxing é considerada um abuso cujo objetivo é danificar uma das partes com a digulvação de dados e informações sensíveis e suas motivações são variadas: desde razões pessoais até políticas. (SNYDER et al, 2017). De acordo com Fox-Brewster (2014), logo que a página foi retirada do ar, o indivíduo com acesso aos servidores, conhecido pelo apelido online de “nachash”, vazou os registros do site na esperança que outros pudessem identificar os meios pelos quais as autoridades policiais capturaram o domínio. No entanto, apesar de ter confiscado o domínio, o conteúdo dos servidores permanece-se ao alcance dos colaboradores do site Doxbin – bastando “apenas” que configurem um domínio para acesso do público. (FOX-BREWSTER, 2014).

Do total de 25 atores presentes no banco de dados desta pesquisa, 5 correspondem por 80% do número de ocorrências totais. O Tor Project corresponde por cerca de 35% por total de ocorrências, seguidos pelo mercado online Silk Road e sua versão posterior, Silk Road 2.0. O ex-agente da NSA, Edward Snowden, responde por cerca de 8% das ocorrências, enquanto que o mercado online Alphabay cerca de 7% do total.

GRÁFICO 3 - TOP 5 ATORES POR PERCENTUAL DE OCORRÊNCIAS (2007-2017)



4.3 DIFUSÃO DE PODER: ATORES, GRUPOS TEMÁTICOS E OCORRÊNCIAS TOTAIS

Nossa análise de difusão de poder foi realizada a partir das três dimensões definidas – autoridade, controle e resultados. Cada dimensão teve análise própria, uma vez que as dimensões são distintas e as variáveis (de mesmo nome) operam em escalas diferentes.

A análise foi realizada em três recortes: primeiro, no nível dos atores – em que cada ator foi analisado de modo individual a partir das ocorrências em que é protagonista; segundo, no nível dos grupos temáticos – momento em que reuniu-se o conjunto de atores com temas similares e analisou-se as ocorrências totais do grupo; e, terceiro, de modo geral – as análises foram realizadas a partir de todas as ocorrências oriundas do período entre 2007-2017. Com isto, buscou-se fornecer um diagnóstico da difusão de poder segundo publicações jornalísticas do período supracitado acerca da rede anônima de baixa latência TOR – de modo a responder a nossa pergunta de pesquisa.

Ressaltamos que a análise individual por ator fornece insumo suficiente para identificar o ator preponderante dentro de cada grupo temático. A tabela geral contendo as análises de cada dimensão por ator, grupo temático e ocorrências totais encontra-se no apêndice desta dissertação.[161]

4.3.1 Dimensão "Autoridade"

O grupo temático com maior número de ocorrências é Online Marketplace (57 ocorrências ou 40,7% do total). Na dimensão **autoridade**, verificamos que houve decrescimento da autoridade dos atores que compõem o grupo em 47 ocorrências. Nas 10 ocorrências restantes houve empate: em 5 ocorrências a autoridade permaneceu estável, e em outras 5 houve crescimento da autoridade. No total, percebemos que houve mais decrescimento da autoridade dos atores que compõem o grupo "Online Marketplace" do que estabilidade ou crescimento. Cabe lembrar que os atores que compõem este grupo são os "mercados negros" anônimo da rede de baixa latência TOR – responsáveis por administrar um espaço de encontro entre vendedores e compradores de produtos ilícitos, agindo como promotores de transações comerciais de drogas e entorpecentes, principalmente.

Existem duas hipóteses que explicam o decrescimento da autoridade destes atores que operam via rede anônima. A primeira hipótese é que os jornais selecionados para esta pesquisa priorizam a publicação de notícias que constatam a prisão dos administradores responsáveis pelos mercados negros, ou o fechamento do domínio do mercado online na rede anônima – ou seja, o acesso público aos mercados pelo TOR. A segunda hipótese é que, de fato, mais fechamentos e prisões estão acontecendo do que proliferação de mercados anônimos e casos de sucesso – ou seja, aqueles que operam livremente via TOR, sem a interferência de autoridades policiais.

Seja como for, o declínio da autoridade dos mercados anônimos reflete a "desconfiança" dos pares e interessados (clientes do mercado, cidadãos privados interessados em consumir os produtos vendidos e indivíduos interessados em administrar mercados semelhantes e auferir ganhos proveniente da comissão de vendas) sobre os mercados em

161 Verificar "Apêndice 9 – Análise de Difusão de Poder por Ator e Grupo".

questão. Se as notícias publicadas refletem prisões e fechamentos de mercados anônimos, a autoridade destes não se mantém estável ou crescentes no tempo – pelo contrário, demonstra declínio. Este declínio é reflexo da relação de poder entre a autoridade do Estado e a autoridade dos mercados anônimos: enquanto estes vêm sua autoridade declinar (devido aos fechamentos dos mercados e prisões dos administradores), aqueles observam sua autoridade crescer perante a sociedade pois alcançam os resultados que eles próprios objetivavam. Portanto, a partir das ocorrências analisadas, oriundas dos artigos de notícias publicados pelos dez maiores jornais em número de usuários por clique, podemos afirmar que o poder dos mercados online que operaram na rede anônima TOR entre os anos de 2007 a 2017, na dimensão autoridade (que diz respeito a confiança dos pares e interessados), sofreu mais declínio que estabilidade ou crescimento.

O segundo grupo temático com maior número de ocorrências, 54, é o grupo "Surveillance Circunvention". Verificamos que a maior parcela destas ocorrências reflete crescimento ou estabilidade da autoridade dos atores que compõem o grupo. Em 27 ocorrências houve crescimento de autoridade; em 18 ocorrências verificou-se que a autoridade manteve-se estável; somente em 9 ocorrências houve declínio da autoridade. A estabilidade e o crescimento da autoridade do grupo reflete o sucesso de atores não-estatais tanto em burlar, por meio da rede anônima TOR, o regime de censura no domínio digital imposto por países autoritários como China e Irã, quanto em manter o anonimato de suas identidades e operações. Em especial, o destaque do ator Tor Project que, através da manutenção e aprimoramento da rede, bem como adoção de técnicas pertinentes ao ativismo em geral, foi o grande responsável por oferecer canal de comunicação alternativo de navegação na Internet. O aumento da autoridade de atores não-estatais, ou, pelo menos, a estabilidade desta autoridade, parece refletir a dificuldade dos Estados em geral em dar continuidade ao regime de censura e bloqueio de regiões cibernéticas para acesso público. Portanto, a partir das ocorrências analisadas, podemos afirmar que o poder, na dimensão **autoridade** (que reflete a confiança e interesse dos pares), de atores que oferecem canal de comunicação alternativo à censura e bloqueio imposto por rígidos mecanismos estatais, aumentou durante o período entre 2007 e 2017.

O terceiro grupo temático por ordem de ocorrências é "Journalism & Whistleblowing", com 21 ocorrências apuradas. Assim como o grupo temático anterior, verificamos que os atores deste grupo

têm tido crescimento na **autoridade**, ou, pelo menos, estabilidade. Em 16 ocorrências verificou-se crescimento da autoridade e em 5 ocorrências estabilidade. Em nenhuma ocorrência constatou-se declínio da autoridade de algum ator do grupo, seja denunciante, jornalista ou grupo ativista que atuam com informações sensíveis. Dentro do grupo, o destaque deu-se a Edward Snowden, com 11 ocorrências, dentre as quais 9 refletiram crescimento da autoridade e 2 delas estabilidade. As revelações de Snowden detalhavam, por meio de arquivos e documentos oriundos da NSA, a vigilância digital massiva perpetrada pelo governo dos EUA e demais aliados. A partir da leitura dos artigos, verificou-se o aumento da confiança depositada na figura do denunciante por pares e interessados – inclusive por ter sido formalmente parte operante do esquema de vigilância.

Neste sentido, a partir da análise das ocorrências feitas acerca do grupo "Journalism & Whistleblowing", podemos afirmar que houve aumento do poder destes atores não-estatais na dimensão autoridade. Uma hipótese para ausência de decrescimento da autoridade destes atores é de que a rede anônima TOR, no período analisado, providenciou meio de comunicação seguro para que denunciantes de grande relevância pudessem transmitir a jornalistas e demais profissionais que lidam com informações sigilosas documentos e arquivos que comprovam as denúncias. Ou seja, a rede anônima de baixa latência TOR ofereceu canal de comunicação visto como suficientemente seguro a ponto de atrair denunciantes de alto risco – seja por sua posição dentro do aparato governamental, seja pelo teor sigiloso das informações em sua posse. Além disso, também serviu como meio receptor de informações sigilosas por parte do corpo editorial de jornais convencionais e organizações ativistas.[162] Por esta razão, denunciantes, jornais e organizações ativistas viram a confiança depositada em si por pares e interessados aumentar no período investigado.

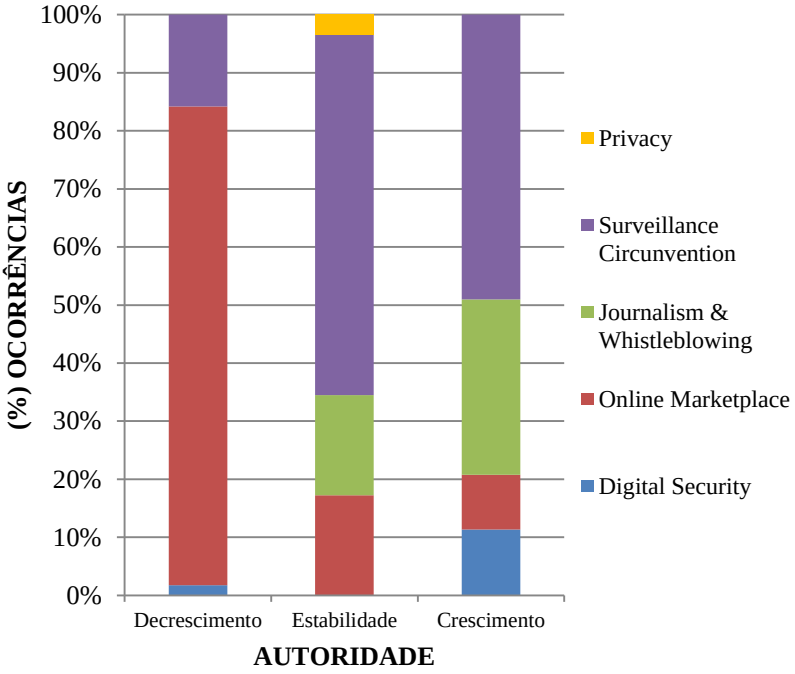
O quarto grupo temático, "Digital Security", é responsável por 7 ocorrências analisadas. Cada ator do grupo foi responsável por 1 ocorrência, totalizando 7 atores e 7 ocorrências. Com exceção do ator

162Além de Edward Snowden, outros denunciantes que apareceram nas ocorrências analisadas foram Chelsea Manning, responsável por transferir documentos secretos das forças armadas norte-americanas à organização WikiLeaks, e Harold T. Martin, que assim como Edward Snowden, também trabalhou para a empresa Allen Booz Hamilton que fornecia serviços para a NSA. Já a organização WikiLeaks, o grupo ativista X-Net Group, jornal The Guardian (SecureDrop System) , The New Yorker (Strongbox) e ProPublica oferecem canal de comunicação e envio de documentos, através da rede anônima TOR, para que denunciantes possam realizar suas denúncias.

Freedom Hosting, verificou-se crescimento da autoridade nos demais atores. Ao sofrer infiltração de malwares, que acredita-se ter sido implantada por agentes do FBI, o servidor Freedom Hosting, acessível somente pela rede anônima TOR, permitiu o acesso das autoridades às informações alocadas nele. Cabe lembrar que o servidor hospedava arquivos e documentos em grande parte referentes à pornografia infantil. Por esta razão, a autoridade do servidor Freedom Hosting sofreu queda, visto que a confiança dos pares e interessados em alocar e acessar informações nele entra declínio devido ao receio da descoberta das identidades por trás dos usuários visitantes. Os demais atores compreendem softwares maliciosos, pesquisadores e profissionais de segurança digital que operam na rede anônima – estes viram a confiança depositada em si por pares e interessados aumentar.

O quinto e último grupo "Privacy" compreende uma única observação de um único ator, a página Doxbin responsável por reunir em um único local a exposição de dados privados de indivíduos. Verificou-se que não houve crescimento ou decrescimento da autoridade desta página, e sim estabilidade da autoridade. Ou seja, a confiança dos pares e interessados não aumentou, nem diminuiu, apenas manteve-se.

GRÁFICO 4 - (%) OCORRÊNCIAS POR GRUPO TEMÁTICO NA DIMENSÃO AUTORIDADE (2007-2017)



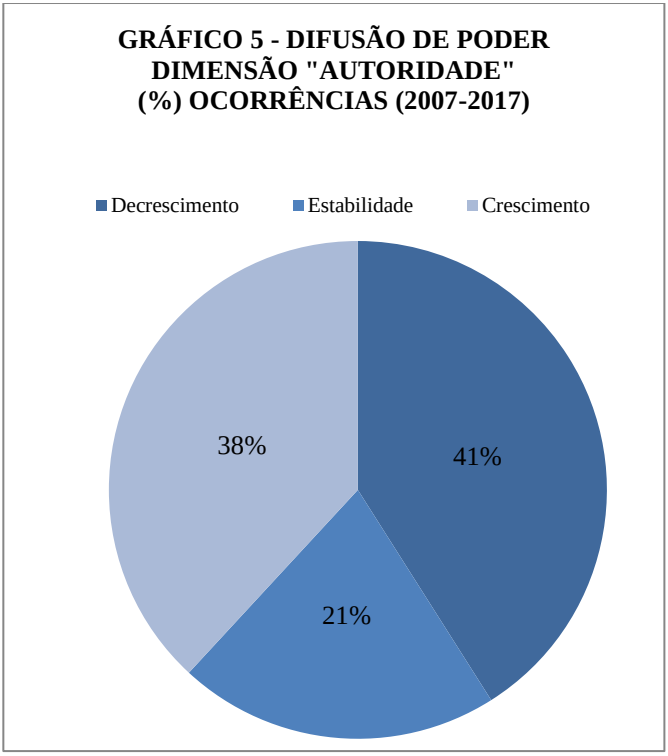
Por meio do gráfico de percentual da difusão de poder na dimensão autoridade é possível realizar algumas interpretações comparativas entre os grupos temáticos

Dentre todos os grupos temáticos, aquele com maior percentual de decrescimento de autoridade é o grupo "Online Marketplace". De fato, a partir dos artigos jornalísticos analisados nesta pesquisa, verificou-se que sua maior parte expôs dois grandes assuntos – aqueles relativos a prisão e julgamento dos administradores por trás dos mercados anônimos, e aqueles relativos ao fechamento do domínio por parte de autoridades policiais. Ambos os assuntos incidem no grau de confiança depositado nos mercados que operam na rede anônima TOR e diminuem a autoridade destes perante os pares e interessados.

O grupo "Surveillance Circunvention" é aquele com maior percentual de estabilidade e crescimento da autoridade. Os artigos de

jornais analisados evidenciaram, principalmente, duas consequências das operações do ator Tor Project, responsável pela manutenção e melhoria da rede anônima. A primeira consequência refere-se à censura e bloqueio de conteúdos no domínio cibernético por parte de Estados autoritários. O Tor Project oferece alternativa de acesso aos conteúdos proibidos, tornando-se importante aliado de ativistas e denunciantes em regiões cujas informações buscam ser controladas por governos. A segunda refere-se a proteção do conteúdo das mensagens trocadas pela rede anônima e a proteção da identidade dos usuários que operam na rede. Estas proteções driblam o sistema de vigilância perpetrado, principalmente, por atores governamentais. Por estas razões, a confiança depositada, por pares e interessados, na organização ativista Tor Project tem crescido – o que é refletido na análise.

Ressalta-se, ainda, o grupo temático "Journalism & Whistleblowing" que configura-se como segundo grupo com maior crescimento percentual da autoridade – atrás somente do grupo "Surveillance Circunvention". O crescimento da autoridade reflete o aumento da confiança depositada por pares e interessados nos atores do grupo por utilizarem a rede anônima como canal de transmissão de informações sensíveis – visto que a rede oferta proteção a privacidade e anonimato dos usuários.



O gráfico acima diz respeito a todas as ocorrências entre 2007-2017 que foram analisadas por esta pesquisa, sem identificar atores ou grupos temáticos.

É possível observar que na dimensão "autoridade", a maior percentagem das ocorrências analisadas nesta pesquisa refere-se ao decrescimento da autoridade dos atores não-estatais. A segunda maior percentagem das ocorrências indica que houve crescimento da autoridade dos atores-não estatais, enquanto que 21% das ocorrências aponta para a estabilidade de autoridade. No entanto, se admitirmos que a difusão de poder ocorre a partir do não-decrescimento das autoridades não-estatais, então podemos considerar que a difusão de poder, neste caso, é fruto do percentual de crescimento e, no máximo, de estabilidade da autoridade. Ou seja, no mínimo, o ator não-estatal que já possuía algum grau de autoridade conseguiu manter este grau, ao passo que aquele que não tinha nenhum grau de autoridade, viu sua autoridade

crescer – ou melhor, sair de *nenhuma* autoridade para *alguma* autoridade. Este cenário é diferente daquele em que apenas considera-se o crescimento da autoridade, pois naquele, exclui-se da análise todos os demais atores não-estatais que *já possuíam* algum grau de autoridade. Por esta razão, podemos pensar que a difusão de poder está ocorrendo a partir do momento em que, no mínimo, verifica-se um ator não-estatal com algum grau de autoridade sobre matérias derivadas do conjunto de valores oriundos da organização social.

Sendo assim, no conjunto das ocorrências analisadas por esta pesquisa, observamos que em cerca de 59% delas a autoridade do ator não-estatal, pertencente à estrutura do conhecimento, cresceu ou pelo menos não diminuiu em razão do uso da rede anônima de baixa latência TOR.

4.3.2 Dimensão "Controle"

Na dimensão **controle**, nota-se que todos os atores da categoria "Online Marketplace" detiveram algum grau de controle sobre objetos relevantes – neste caso, o próprio mercado online e mecanismos de pagamentos. Em 29 ocorrências observou-se o controle parcial do mercado anônimo sobre o espaço virtual de encontro entre compradores e vendedores e o sistema de pagamentos utilizados por eles para efetuar a transação comercial. Em 28 ocorrências observou-se o controle absoluto dos mercados anônimos. Não houve casos em que o controle foi considerado "nenhum".

Nos artigos de notícias publicados sobre o tema, em boa parte verifica-se o controle absoluto do mercado online. Nestas ocorrências, o controle do mercado é absoluto pois ele é responsável por fornecer o espaço virtual de encontro entre compradores e vendedores e também o sistema de pagamentos na sua totalidade – dispensando a presença de terceiros, como bancos ou bandeiras de cartões, etc. O sistema de pagamentos, neste caso, é baseado em moeda virtual criptográfica (geralmente Bitcoins) e depende da aprovação do(s) responsável(eis) para que a transação financeira entre vendedor e comprador seja efetuada.[163] A posse do controle do ambiente

163Mecanismo conhecido como "escrow", detalhado anteriormente. O administrador do mercado online, depois da confirmação de ambos vendedor e comprador sobre o pagamento e recebimento da mercadoria comprada, autoriza a transação definitiva do pagamento em moeda criptográfica, colhendo para si uma parcela da quantia (comissão).

virtual do mercado permite que o mesmo tenha poder de permitir ou negar o acesso das partes interessadas nas transações comerciais. Caso o responsável pelo mercado tenha o controle de ambos – espaço virtual de encontro entre compradores e vendedores e sistema de pagamentos, – é dito que ele têm o controle absoluto sobre a operação do mercado anônimo. Caso o responsável pelo mercado tenha apenas o controle do espaço virtual, e não do sistema de pagamentos, afirmamos que o controle sobre o objeto é parcial – pois uma parte do controle das operações do mercado anônimo está a disposição de outra entidade ou instituição.[164]

Assim como o grupo anterior, no grupo "Surveillance Circunvention", todos os atores detiveram algum grau de **controle** sobre objetos relevantes para a execução de suas atividades. O destaque é o controle absoluto do funcionamento da rede anônima TOR por parte do ator Tor Project – responsável por sua administração, manutenção e melhoria. A partir da análise das ocorrências, verificou-se que o Tor Project tem o controle absoluto sobre a remoção de qualquer nódulo suspeito da rede anônima – o que aconteceu em algumas ocasiões. Além disso, o Tor Project também tem o controle sobre a criação de "bridges" que permitem o acesso à rede por usuários que encontrem-se, de alguma maneira, bloqueados de acessar a rede por meios padronizados.

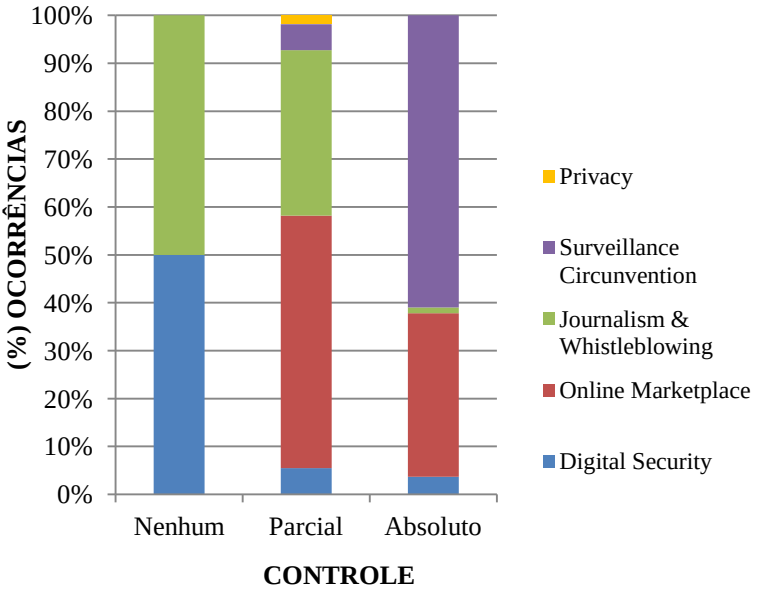
Observando os dados de difusão do grupo "Journalism & Whistleblowing" é possível perceber que a maioria dos atores que o compõem detiveram algum grau de controle sobre objetos considerados relevantes para o alcance dos resultados desejados. Este controle foi, majoritamente, parcial – com 19 das ocorrências (de um total de 21 ocorrências).

No grupo "Digital Security", verificou-se que a maior parte dos atores que compõem o grupo têm algum grau de **controle** sobre objetos pertinentes ao alcance de seus objetivos operados pela rede anônima TOR. Estes objetos variam desde servidores localizados na rede até a própria rede anônima. Do total de 7 ocorrências, os atores têm controle parcial sobre objetos em 3 ocorrências; e controle absoluto em outras 3 ocorrências. O único ator sem controle nenhum de objeto relevante à operação de suas atividades é o especialista em segurança Dan Egerstad, que observou brechas de segurança de embaixadas na rede anônima.

Em relação ao grupo "Privacy", a partir da ocorrência analisada, foi possível identificar que o ator detinha **controle** parcial sobre os servidores que contêm o conjunto de informações pessoais de inúmeros indivíduos.

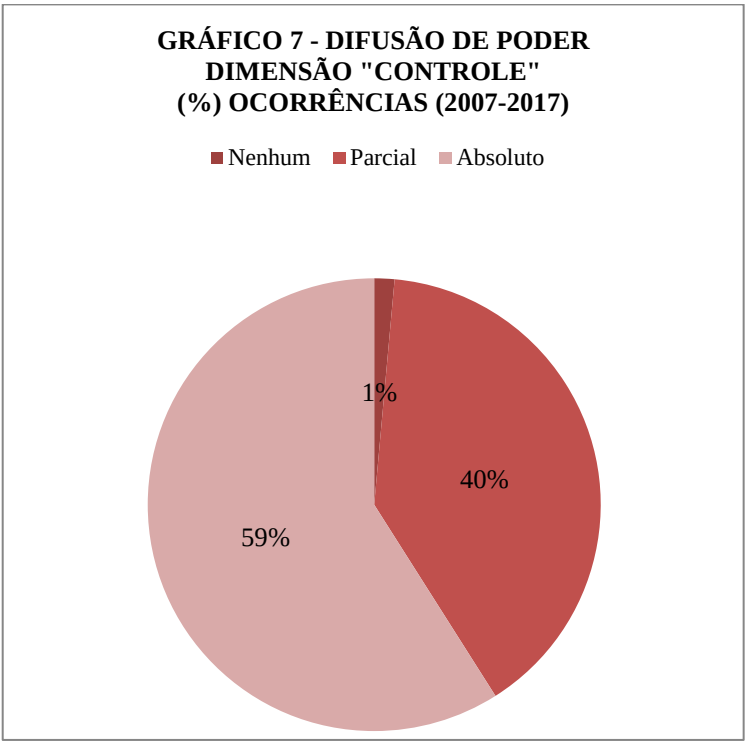
164A interpretação do controle absoluto ou parcial do mercado anônimo é oriunda das ocorrências analisadas: caso esteja explícito que o mercado anônimo opera com sistema de pagamentos próprio, dizemos que o controle é absoluto. Caso não esteja explícito, dizemos que o controle do mercado anônimo é parcial.

GRÁFICO 6 - (%) OCORRÊNCIAS POR GRUPO TEMÁTICO NA DIMENSÃO CONTROLE (2007-2017)



Se observamos dados estatísticos que comparam percentuais dos grupos temáticos entre si, na dimensão do controle, observamos que os grupos temáticos "Journalism & Whistleblowing" e "Digital Security" foram aqueles que menos apresentaram controle sobre algum objeto relevante às suas operações em termos percentuais. Ambos os grupos tiveram uma única ocorrência para "nenhum" controle. Já o grupo "Online Marketplace" foi aquele que mais obteve controle parcial sobre os objetos (neste caso, os próprios ambientes virtuais de encontro entre compradores e vendedores e o sistema de pagamentos por meio do qual eram realizados as transações financeiras), seguido do grupo "Journalism & Whistleblowing", cujos atores parcialmente controlavam informações, documentos e arquivos sigilosos (no caso de denunciantes) e canais seguros de transmissão e publicação destas informações (no caso de jornalistas e ativistas). O maior percentual de controle absoluto foi relativo ao grupo temático "Surveillance Circunvention", cujo ator

Tor Project é responsável pela manutenção e administração da rede anônima.



Na dimensão “controle”, observamos pelo gráfico que em 59% das ocorrências analisadas nesta pesquisa, o ator não-estatal oriundo da estrutura do conhecimento deteve o controle absoluto de um objeto enquanto exercicia atividades no domínio cibernético. Em 39% das ocorrências, este controle foi parcial; enquanto que em apenas 2% das ocorrências o controle foi nenhum. Em outras palavras, em 98% das ocorrências o ator não-estatal deteve algum grau de controle sobre objetos oriundos da estrutura do conhecimento durante suas operações na rede anônima TOR.

4.3.3 Dimensão “Resultados”

Na dimensão **resultado**, na maior parte das ocorrências (42 ocorrências) dos atores do grupo “Online Marketplace” foi possível observar alteração do status-quo com efeitos sobre a realidade. Em apenas 15 ocorrências verificou-se a não-alteração do status-quo, ou seja, sua manutenção. Em outras palavras, as ocorrências analisadas forneceram insumos suficientes para afirmar que em razão do uso da rede anônima de baixa latência TOR, os mercados onlines que operam nesta rede conseguiram efetivar a comercialização de substâncias ilícitas, como drogas e entorpecentes no geral, no plano real.

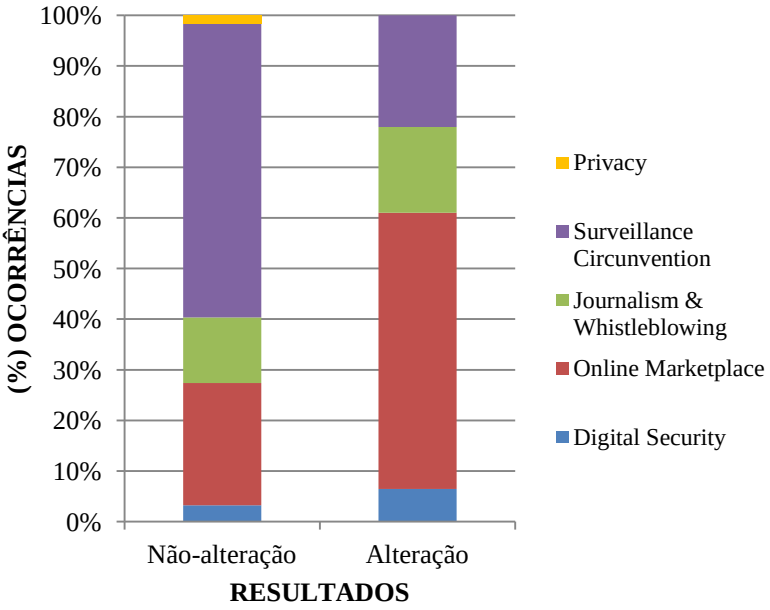
No grupo “Surveillance Circunvention”, observa-se que, na dimensão **resultado**, não houve alteração do status-quo no plano real na maior parte das ocorrências. O status-quo em questão reflete duas situações: primeiro, a manutenção do bloqueio e censura de determinados conteúdos na Internet por parte de países autoritários; segundo, a manutenção do anonimato das operações e identidades dos usuários que utilizam a rede anônima TOR. A primeira situação reflete um número reduzido de ocorrências, enquanto a segunda situação reflete a maior parte das ocorrências analisadas. Em cerca de 65% das ocorrências não houve alteração dos status-quo mencionados acima; enquanto que em cerca de 35% das ocorrências, houve alteração destes status-quo.

No que tange o grupo “Journalism & Whistleblowing”, é possível afirmar que houve alteração do status-quo, com consequências para o plano real, na maior parte das ocorrências: 13 alterações de stats-quo frente a 8 ocorrências de não-alteração.

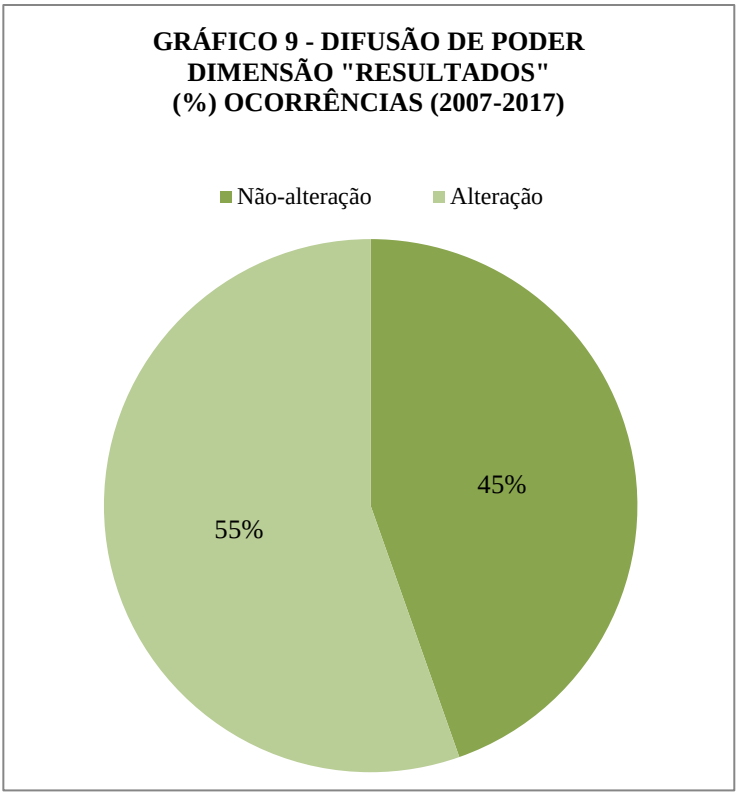
No grupo “Digital Security”, em 70% das ocorrências deste grupo temático houve alteração do status-quo no plano real geográfico. Em 30% das ocorrências o status-quo manteve-se inalterado.

Em relação ao grupo “Privacy”, não observou-se a partir das ocorrências alteração do status-quo no plano real – evidência de que, apesar de reunir dados e informações pessoais de indivíduos, estas informações não foram utilizadas no plano real para qualquer fim.

GRÁFICO 8 - (%) OCORRÊNCIAS POR GRUPO TEMÁTICO NA DIMENSÃO RESULTADOS (2007-2017)



Na dimensão resultados, verificamos por meio do gráfico percentual de ocorrências que o tema que mais logrou alteração do status-quo, com consequências para o plano real geográfico, foi o grupo "Online Marketplace". A prisão e o julgamento de administradores de mercados online anônimos evidenciam a transação comercial de substâncias ilícitas, drogas e entorpecentes por meio da rede de baixa latência TOR. De modo geral, como constatado por Sedghi (2014), houve um aumento do consumo destas substâncias em razão do acesso relativamente seguro aos mercados da rede anônima. O grupo temático que menos logrou alteração do status-quo no plano real foi "Surveillance Circunvention". A hipótese é que a blindagem frente a vigilância perpetrada no domínio cibernético seja um ato passivo, ou seja, apenas incidirá sobre o status-quo caso a entidade responsável pela vigilância logre e haja sobre o indivíduo a quem vigia-se – e não o contrário.



Em relação a última dimensão, “resultados”, foi possível verificar que em 56% das ocorrências analisadas por esta pesquisa houve alteração do status-quo com consequências para o plano real geográfico. Ou seja, em mais da metade das ocorrências os atores não-estatais lograram sucesso na alteração do status-quo em razão do uso da rede anônima de baixa latência.[165]

165 A exceção do ator Tor Project, podemos dizer que os atores que logram sucesso na alteração do status-quo agem no sentido de alcançar os resultados desejados. Já o ator Tor Project atua com o propósito de não-alteração do status-quo no plano real uma vez que esta organização (responsável por realizar manutenções e melhorias na rede) busca a proteção da privacidade e o anonimato dos usuários e das mensagens trocadas. A

4.3.4 Análise de Difusão de Poder no Contexto da Rede Anônima TOR

Acreditamos que existem indícios suficientes para acreditar que a difusão de poder atua em três dimensões distintas. Podemos afirmar que a difusão de poder está em curso quando há o crescimento de autoridades não-estatais (ou pelo menos a manutenção das autoridades não-estatais já existentes); quando atores não-estatais são capazes de controlar objetos relevantes para o alcance dos fins desejados; e quando estes, por meio de suas ações, logram alterar o status-quo – cujas consequências incidem sobre o plano real geográfico (vez que nesta pesquisa versamos sobre as atividades e operações de sujeitos no domínio cibernético). As três dimensões denotam poder pois corroboram com o quadro analítico proposto por Strange (1988) que culminou no campo da EPI. Embora ela própria não tenha versado sobre as três dimensões, quando analisamos o fenômeno de difusão de poder por meio destas dimensões, somos capazes de averiguar sua existência ou ausência.

Esta afirmação deriva da seguinte lógica: quando existe concentração de poder na figura do Estado – ou seja, o oposto da difusão de poder definida por Strange (1996) – isto significa, para as três dimensões, que (1) o Estado tem a liderança de autoridade em matérias derivadas dos valores oriundos da organização social – o que inclui a estrutura do conhecimento; (2) o Estado é aquele que mais detém o controle sobre objetos pertinentes ao alcance de resultados desejados por ele; (3) o poder do Estado é de tal maneira que logra alterar o status-quo, ou seja, é capaz de alcançar os objetivos que almeija. A difusão de poder reflete nestas três dimensões a lógica contrária: o Estado não detém a liderança nas estruturas primárias (e, neste caso, na estrutura do conhecimento); ele não é o único com capacidade de controlar objetos relevantes para a consecução dos objetivos propostos; e não é o único capaz de realizar alterações no status-quo. Entretanto, cabe ressaltar que esta dissertação é de caráter exploratório, ou seja, não tem pretensão de

---

alteração no status-quo indica, por vezes, que o anonimato dos usuários e mensagens não teve efetividade.

oferecer respostas fixas sobre tema desafiador, embora pondere sobre pontos específicos da literatura.

Em suma, observamos a difusão de poder ocorrer nas três dimensões para a maior parte dos atores não-estatais posicionados na estrutura do conhecimento que realizaram suas operações via rede anônima de baixa latência TOR.

4.3 CONCLUSÃO

Este capítulo buscou realizar uma análise da difusão de poder em três dimensões. Esta análise incidiu-se sobre banco de dados confeccionado a partir de artigos jornalísticos provenientes dos dez maiores jornais do mundo em número de ususários por clique. Este banco de dados trouxe atores não-estatais, posicionados dentro da estrutura do conhecimento, como protagonistas de ações perpetradas via rede anônima de baixa latência "The Onion Router". Esta rede tornou-se conhecida por oferecer um canal de comunicação alternativo no domínio cibernético – alheio às autoridades governamentais – que visa assegurar a privacidade dos usuários e o anonimato das mensagens trocadas por ela. A tecnologia desenvolvida pela organização responsável pela rede TOR é oriunda de conhecimentos e informações sobre técnicas criptográficas e de roteamento, entre outros, que acumularam-se principalmente durante os anos 1990. Esta rede ficou especialmente conhecida pelo público geral após os anos 2013 e 2014, momento em que veículos midiácitos publicaram notícias relacionadas aos mercados anônimos que nela operam, bem como prisões e julgamentos dos seus responsáveis, além de ser comumente associada a denunciantes e jornalistas em razão da proteção que assegura às comunicações.

A partir da fundamentação conceitual sobre a rede anônima TOR como importante parte da estrutura do conhecimento no século XXI, explorada no capítulo dois, nós buscamos apresentar o método por meio do qual elaboramos o banco de dados utilizados nesta pesquisa. Este banco de dados foi fruto de investigações sobre artigo de notícias publicados por 22 jornais, no total, e oriundos de quatro países: Estados Unidos, Inglaterra, Índia e China. Por meio de cada artigo de jornal, buscamos identificar atores não-estatais posicionados na estrutura do conhecimento, bem como suas ações realizadas via rede anônima TOR. A composição do banco de dados desta pesquisa resultou em 139 linhas e 14 colunas, e nos permitiu identificar 25 atores, que reunimos em 5 grupos temáticos – uma vez que foi possível identificar temas similares nos artigos jornalísticos. A partir das informações dispostas, pudemos realizar as análises de difusão de poder em três dimensões e segundo aporte teórico apresentado no primeiro capítulo desta dissertação.

Nossa análise de difusão de poder, além de compreender as três dimensões, visou a exposição de três recortes, como modo de fornecer uma visão sistemática sobre o banco de dados. Estes três recortes foram sobre: os atores, os grupos temáticos e sobre as ocorrências totais entre

os anos de 2007 e 2017. De modo geral, nós pudemos observar que, na dimensão autoridade, a rede anônima TOR contribuiu para o aumento – ou pelo menos estabilidade – de autoridade dos atores na maior parte das ocorrências. Na dimensão controle, nós identificamos que quase a totalidade dos atores não-estatais dispuseram-se do controle sobre objetos no domínio cibernético. Estes objetos foram pertinentes para o alcance dos resultados desejados por eles. Em outras palavras, nós verificamos que a maior parte dos atores não-estatais detinham algum grau de controle sobre objetos no ensejo de suas operações. E estes objetos, que operam no domínio cibernético, são construções abstratas frutos de conhecimento acumulado oriundos, em nossa análise, da sociedade civil. O domínio destes objetos por parte dos atores não-estatais em nossa análise demonstra a relevância do conhecimento e das informações no ciberespaço – o que nos leva supor que a dimensão cibernética é importante domínio para a estrutura do conhecimento no século XXI. Na dimensão resultados, foi possível observar que em mais da metade das ocorrências, os atores não-estatais lograram a alteração do status-quo com consequências para a realidade geográfica (ou seja, não-cibernética).[166] Este sucesso em alterar os resultados aconteceu em razão do uso da rede anônima TOR que, por sua tecnologia e natureza, permite a dinâmica através do qual os atores operaram de modo a alcançar estes resultados.

Em suma, a rede anônima TOR contribui para a difusão de poder nas três dimensões a partir de suas especificidades tecnológicas que diferem de outros canais de comunicação. Em nossa análise, esta difusão de poder foi evidenciada na maior parte das ocorrências do banco de dados utilizado por nós para fins desta pesquisa. Cabe ressaltar que este banco de dados é fruto de abordagens jornalísticas que visam notificar o público acerca de questões de relevante interesse geral. Foi por meio da rede TOR que diversos atores puderam realizar suas operações de modo a incidir sobre o status-quo. Sendo assim, ressalta-se a diferença entre a Dark Web e a Surface Web para fins de resultados e para a difusão de poder. Há razões para acreditar que os atores analisados nesta pesquisa não teriam logrado os mesmos resultados caso houvessem operado por outros canais de comunicação com tecnologia e natureza diferente da rede anônima – como por exemplo a Surface Web.

[166] À exceção do ator Tor Project.

CONSIDERAÇÕES FINAIS

A disciplina de Economia Política Internacional ganhou relevância nos estudos em Relações Internacionais por, paradoxalmente, ofertar uma abordagem sobre o Sistema Internacional que inclui atores não-estatais. A britânica susan Strange inaugura a visão sobre atores, atividades e indivíduos no SI a partir de uma ótica que busca responder questões político-econômicas a partir de quatro estruturas primárias. Esta nova abordagem inclui atores não-estatais e aproxima os estudos acadêmicos da realidade prática, afinal, embora os Estados sejam aqueles responsáveis por, em última análise, sustentar a ordem e a segurança dentro dos territórios nacionais, eles não podem ser considerados as únicas autoridades que incidem sobre as pessoas e os serviços.

Embora não seja teórica, Strange (1988) foi uma acadêmica e erudita que proporcionou uma visão sobre as operações do tecido político-econômico internacional de modo a abranger quatro estruturas que, de acordo com ela, encontram-se no cerne de qualquer sociedade, seja de nível global ou local: segurança, produção, finanças e conhecimento. Afinal, todas as sociedades minimamente organizadas preocupam-se com a segurança e a sobrevivência; com a produção de alimentos, ferramentas, produtos em geral; com a criação do crédito; e com o acúmulo de conhecimento e informações que possam ser passadas adiante entre as gerações. O sistema internacional é observado, portanto, a partir de um quadro analítico que permite a atuação de outros atores além do Estado – uma vez que estes não são os únicos que incidem sobre as quatro estruturas e sobre as pessoas. O paradigma da EPI de Strange visa compreender o modo pelo qual o poder opera no tecido sócio-político-econômico e, por esta razão, teceu críticas tanto a economistas (por ignorarem o elemento do poder em suas análises) quanto cientistas políticos (por ignorarem aspectos importantes da economia). Este novo paradigma busca fornecer recursos suficientes para análises que acobertem ambos os segmentos dentro de um contexto global, ou melhor, internacional.

É a partir do paradigma da EPI abordada na obra de 1988 que Strange colhe as bases que sedimentam sua visão sobre difusão de poder, afirmando que o poder do Estado tem declinado, no sentido qualitativo, em razão da ascensão de outras autoridades agindo globalmente. Segundo ela, tais autoridades têm poder suficiente para não apenas alocar valores básicos da organização humana em sociedade, mas

também com capacidade suficiente para alterar os resultados e redefinir opções para os demais. Estas diversas autoridades não-estatais estão amplamente inseridas nas quatro estruturas primárias. Seu poder poder indireto, ou melhor, estrutural é justamente fruto das da ação das dinâmicas estruturais, enquanto que o poder direto é velho conhecido da disciplina de RI: conhecido também por poder relacional.

Nesta pesquisa buscamos analisar a difusão de poder através da rede anônima de baixa latência "The Onion Router". Esta rede opera através da Internet, sendo parte do conjunto de redes que formam a "Dark Web" – região da web em que há esforço ativo para manter o anonimato das comunicações e dos usuários. Esta rede anônima busca ser relevante canal de comunicação frente a vigilância digital perpetrada por entes governamentais e privados. Como meio de comunicação, ela insere-se dentro da estrutura do conhecimento, uma das estruturas primárias definidas inicialmente por Strange em 1988. Segundo ela, além de compreender crenças, princípios e conclusões morais, esta estrutura compreende também o que é conhecido e compreendido como entendido e extende-se também sobre os canais de comunicação por meio do qual a informação é comunicada. Por esta razão, podemos afirmar que a rede anônima de baixa latência TOR faz parte da estrutura do conhecimento. E, como pertencente a estrutura do conhecimento, verifica-se a existência de sujeitos, também posicionados nesta estrutura, que operam na rede anônima. Ora, se Strange (1988) indica que o quadro analítico estrutural pode ser compreendido a partir de uma visão tanto global, quanto local, não há razão para supor que seja inviável a utilização deste quadro para observações no domínio cibernético. Afinal, diferentes atores estatais e não-estatais operam no ambiente ciber incidindo-se sobre pessoas e serviços ofertados nesta região, muito embora ela própria não tenha versado especificamenete sobre este domínio.

Esta dissertação tratou de responder a pergunta de pesquisa de modo a verificar de que modo, e em que medida, a rede anônima The Onion Router contribui para a difusão de poder na estrutura do conhecimento. Como visto, tanto a estrutura do conhecimento quanto o fenômeno da difusão de poder foram elementos definidos por Strange (1988, 1996) e, por esta razão, nossa pesquisa baseou-se em suas obras durante a investigação do fenômeno neste canal de comunicação específico do plano cibernético. Após considerável exame sobre as obras, identificamos dois pontos relevantes que incidem sobre nossa análise: primeiro, a constatação de que a difusão de poder opera em três

dimensões; segundo, mesmo que não tenha versado sobre o domínio cibernético, Strange indicou a importância das revoluções tecnológicas que ocorriam ao final da década de 1980 e 1990.

A primeira dimensão é a da "autoridade". Nesta dimensão, nós buscamos demonstrar que as considerações de Strange acerca do poder é tratada, por vezes, como considerações acerca da autoridade. No entanto, embora as diferenças entre "poder" e "autoridade" sejam sutis, nós acreditamos que há indicativos suficientes nas obras da autora para afirmar que estes dois elementos não são sinônimos. A autoridade pode ser encarada de duas formas: como entidade que reúne a confiança dos pares e interessados sobre si; e, também, como o próprio exercício de poder. No primeiro momento, nos referimos ao "ser autoridade" – o que pode ser realizado por meio de transferência, outorga, concessão, delegação, etc. Esta autoridade, portanto, pode surgir de modo formal ou informal. No segundo momento, referimo-nos a "exercer autoridade". Este exercício de autoridade implica o uso do poder, afinal, exercer autoridade significa que a autoridade utiliza-se de todos os meios cabíveis a ela para por em prática os fins desejados. Em outras palavras, a autoridade exercer poder de modo a concretizar sua vontade. Ressaltamos, no entanto, que ambas autoridades podem ser testadas, averiguadas, examinadas apenas através da terceira dimensão – resultados.

A segunda dimensão refere-se ao "controle". Inicialmente, nós verificamos que em diferentes ocasiões das obras analisadas, Strange (1988) indica o controle de um objeto por parte de um ator para indicar o seu poder. Nós reunimos as citações em que a autora realiza estas afirmações e identificamos, tanto o ator em questão, quanto o objeto por ele controlado e demos origem ao "APÊNDICE 3" desta dissertação. Isto nos deu insumo suficiente para examinar o papel do controle sobre a conferência de autoridade e poder a atores dentro de uma estrutura. No caso da estrutura do conhecimento, o papel do controle demonstrou ser essencial uma vez que encontra-se no cerne da definição sobre poder na estrutura do conhecimento: o poder é atribuído aqueles que ocupam posição de destaque, ou posição de tomar decisões, na estrutura do conhecimento e recai (1) sobre aqueles reconhecidos pela sociedade como detentores de conhecimento; (2) aqueles responsáveis pelo seu armazenamento; (3) e aqueles que controlam os canais por meio dos quais as informações e conhecimentos são transmitidos. Para fins de análise, nesta dimensão, nós assumimos que o controle pode ser nenhum, parcial ou absoluto.

A terceira dimensão refere-se aos "resultados". Nesta dimensão, os resultados refletem a alteração do status-quo ou a sua manutenção. O resultado atesta, ou refuta, a autoridade de um ator e/ou seu controle sobre objeto que considera pertinente para o alcance do resultado desejado. Ou seja, nós podemos assumir que um ator tem autoridade – afinal, "ser autoridade" demonstra a confiança dos pares e interessados. Esta autoridade não é sinônimo de poder. No entanto, em alguma ocasião, o ator pode exercer a autoridade nele investida (de modo formal ou informal) e alterar o status-quo a favor de cenário desejado por ele. Nesta situação, verifica-se que a autoridade, de fato, tem poder. Mas se o ator, ao exercer a autoridade (ou melhor, poder), não promover a alteração do status-quo a favor de cenário desejado por ele, não podemos admitir que o ator ainda detém autoridade. A autoridade, de fato, apenas pode ser determinada com base nesta dimensão, nos resultados. De modo semelhante, a relevância de um objeto para um determinado ator na busca por um resultado específico apenas pode ser determinado se o controle deste objeto for pertinente para a alteração do status-quo. Caso não seja, o controle deste objeto por parte do ator não resulta em poder.

Nossa busca limitou-se a investigar a difusão de poder no domínio da rede anônima "The Onion Router". Esta investigação ocorreu a partir da elaboração de um banco de dados contendo ocorrências derivadas de artigos jornalísticos. Estes artigos foram oriundos dos dez maiores jornais em número de visitantes por clique, conforme apresentado pela Comscore (2012). O modo por meio do qual os artigos foram selecionados para compor o banco de dados foi apresentado no terceiro capítulo da dissertação. A partir desta composição, nós pudemos realizar algumas interpretações acerca, por exemplo, da popularidade da rede TOR a partir de 2013. Além disso, nós realizamos análises sobre a difusão de poder em três dimensões segundo três recortes distintos: primeiro, apresentamos tabela com a exposição dos 25 atores (oriundos dos artigos jornalísticos); segundo, os atores cujo teor das notícias foram similares e agrupamos no mesmo "grupo temático" e realizamos considerações sobre a difusão para os grupos; e, terceiro, examinamos a difusão de poder por meio do total de ocorrências entre os anos 2007-2017. Através de nossa análise pudemos verificar que a difusão de poder ocorre para a maior parte das ocorrências verificadas. Há indícios suficientes para interpretar que a natureza tecnológica específica da rede anônima TOR é fator

preponderante para a presença do fenômeno na estrutura do conhecimento no século XXI.

Por último, nós também trouxemos considerações importantes sobre o fenônome da difusão de poder sob o paradigma de Nye em relação ao “cyberpower” que origina-se a partir do ciberespaço. O discurso de Nye em relação de poder assemelha-se ao discurso de Strange por tratar-se de um fenômeno “vertical”, em que se supõe que o poder está “diluindo-se” no tecido político e econômico global do Estado em direção a tores não-estatais. Nye também afirma, especificamente, sobre a existência de um poder cibernético (cyberpower), tornando-se o primeiro grande teórico da área de RI a realizar considerações sobre o poder no novo domínio do século XXI. É possível perceber que a definição de poder cibernético, cunhado por Nye (2011), está intimamente relacionado a um conjunto de recursos que derivam da estrutura do conhecimento – ainda que indiretamente.

Finalmente, nós apresentamos gráficos, tabelas e quadros cujo objetivo eram servir de suporte às nossas análises e apresentar as "descobertas" feitas durante esta presente pesquisa.

REFERÊNCIAS BIBLIOGRÁFICAS

ABERYSTWYTH UNIVERSITY (Reino Unido). **International Politics Centenary**. 2017. Disponível em: <https://www.aber.ac.uk/en/interpol/centenary/>. Acesso em: 8 ago. 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. **Anais**. [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: Proxies provide an alternative path to the internet, free of government censorship, as Iranians found during the crackdown. **The Guardian.** London, p. 1-3. 01 jul. 2009. Disponível em: <https://www.theguardian.com/world/2009/jul/01/iran-proxies-bypass-censors>. Acesso em: 25 fev. 2018.

ARTHUR, Charles. The ransomware attack is all about the insufficient funding of the NHS. **The Guardian.** London, p. 1-2. 13 maio 2017. Disponível em: <https://www.theguardian.com/commentisfree/2017/may/13/nhs-computer-systems-insufficient-funding>. Acesso em: 25 fev. 2018.

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

ASSOCIATED PRESS (Estados Unidos). Coldwater man among 15 arrests in international online drug probe. **Michigan News.** Michigan, p. 1-2. 16 abr. 2012. Disponível em: <http://www.mlive.com/news/index.ssf/2012/04/coldwater_man_among_15_arrests.html>. Acesso em: 25 fev. 2018.

ASSOCIATED PRESS (Reino Unido). 'Dark Web' drug site challenge law enforcement. **Daily Mail.** London, p. 1-3. 07 nov. 2014. Disponível em: <http://www.dailymail.co.uk/wires/ap/article-2825613/Europol-17-arrests-major-Darknet-crackdown.html>. Acesso em: 25 fev. 2018.

BACHRACH, Peter; BARATZ, Morton S.. Two Faces of Power. **American Political Science Review,** [s.i.], 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, out. 1995. Cambridge University Press (CUP). http://dx.doi.org/10.1353/wp.1995.0001.

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. Cap. 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 dez. 2012. Informa UK Limited. http://dx.doi.org/10.3109/09687637.2012.745828.

BECKETT, Andy. **The Dark Side of the Internet**: In the 'deep web', Freenet software allow users complete anonymity as they share viruses, criminal contacts and child pornography. 2009. Disponível em: <https://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet>. Acesso em: 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, out. 2006. Wiley-Blackwell. http://dx.doi.org/10.1111/j.1083-6101.2006.00320.x.

BERGHEL, Hal. Which Is More Dangerous—the Dark Web or the Deep State? **Computer**, [s.l.], v. 50, n. 7, p.86-91, 2017. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/mc.2017.215.

BERGMAN, Michael K.. White Paper: The Deep Web. **The Journal Of Electronic Publishing**, [s.l.], v. 7, n. 1, p.1-17, 1 ago. 2001. University of Michigan Library. http://dx.doi.org/10.3998/3336451.0007.104.

BIDDLE, P. et al. **The darknet and the future of content distribution**. 2002. Disponível em: <http://msl1.mit.edu/ESD10/docs/darknet5.pdf>

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, maio 2013. IEEE. http://dx.doi.org/10.1109/sp.2013.15.

BRADBURY, Danny. Chaos aims to crack China's Wall. **The Guardian.** London, p. 1-2. 07 ago. 2008. Disponível em: <https://www.theguardian.com/technology/2008/aug/07/censorship.hacking>. Acesso em: 25 fev. 2018.

BRADBURY, Danny. The problem with Bitcoin. **Computer Fraud & Security**, [s.l.], v. 2013, n. 11, p.5-8, nov. 2013. Elsevier BV. http://dx.doi.org/10.1016/s1361-3723(13)70101-5.

BREWSTER, Tom. Simplelocker Android Malware locks up mobile data and demands a ransom. **The Guardian.** London, p. 1-2. 05 jun. 2014. Disponível em: <https://www.theguardian.com/technology/2014/jun/05/simplocker-android-ransomware-malware-virus>. Acesso em: 24 fev. 2018.

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. Informa UK Limited. http://dx.doi.org/10.1080/14650049808407610.

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. Tese (Doutorado) - Curso de Ciência Política, 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 Yotk: Oxford University Press, 2001. 292 p.

CASTELLS, Manuel; CARDOSO, Gustavo (Orgs.). **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 Securititzação do Ciberespaço e Terrorismo: Uma Abordagem Crítica. In: SOUZA, André de Mello e; NASSER, Reginaldo Mattar; MORAES, Rodrigo Fracalossi de (Org.). **Do 11 de Setembro de 2001 à Guerra ao Terror:** Reflexões sobre o Terrorismo no Século XXI. Brasília: Ipea, 2014. Cap. 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. **Anais**. [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 Chatam House, 2015. 18 p. (Global Comission on Internet Governance).

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. Informa UK Limited. http://dx.doi.org/10.1177/0096340212438696.

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. TCC (Graduação) - Curso de Computer Science And Artificial Intelligence, Division Of Informatics, 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, abr. 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. Springer Berlin Heidelberg. http://dx.doi.org/10.1007/11957454_2

COMPUTER HOPE. Jargon. Disponível em <https://www.computerhope.com/jargon/p/proxyser.htm> Acesso em 4 nov. 2017

CORNISH, Paul et al. **On Cyber Warfare.** London: The Royal Institute Of Internacional Affairs (Chatam House), 2010. 38 p.

CUBRILOVIC, Nik. The Anatomy of the Twitter Attack: Part II. **The Washington Post.** Washington, 18 dez. 2009. p. 1-2. Disponível em: <http://www.washingtonpost.com/wp-dyn/content/article/2009/12/18/AR2009121802393.html24>. Acesso em: 24 fev. 2018.

CURRAN, Giorel; GIBSON, Morgan. WikiLeaks, Anarchism and Technologies of Dissent. **Antipode**, [s.l.], v. 45, n. 2, p.294-314, 22 maio 2012. Wiley. http://dx.doi.org/10.1111/j.1467-8330.2012.01009.x.

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. Wiley-Blackwell. http://dx.doi.org/10.1002/bs.3830020303.

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. Springer Nature. http://dx.doi.org/10.1007/s12117-016-9281-4.

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 out. 2015. Informa UK Limited. http://dx.doi.org/10.1080/19322909.2015.1077183.

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, set. 2007. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/msp.2007.108.

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. ACM Press. http://dx.doi.org/10.1145/1653662.1653708.

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 out. 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. ACM Press. http://dx.doi.org/10.1145/2815675.2815690.

EUROPEAN COUNCIL FOR NUCLEAR RESEARCH (Suíça) (Org.). **About CERN.** 2017. Disponível em: <https://home.cern/about>. Acesso em: 22 set. 2017.

EVERETT, Cath. Moving Across to the Dark Side. **Network Security**. [s.l.], set. 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. Annual Reviews. http://dx.doi.org/10.1146/annurev.polisci.9.060804.162744.

FARRELL, Henry. Why ‘Dark Web’ drug markets will keep on imploding. **The Washington Post.** Washington, p. 1-4. 19 mar. 2015. Disponível em: <https://www.washingtonpost.com/news/monkey-cage/wp/2015/03/19/why-dark-web-drug-markets-will-keep-on-imploding/?noredirect=on&utm_term=.f6846af7c601>. Acesso em: 25 fev. 2018.

FIFIELD, David et al. Evading Censorchip 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. (Congressional Research Service).

FREE HAVENa. **Home**. 2017. Disponível em: <https://www.freehaven.net/index.html>. Acesso em: 24 nov. 2017.

FREE HAVENb. **Overview**. 2017. Disponível em: <https://www.freehaven.net/overview.html>. Acesso em: 24 nov. 2017.

FREENET. **About**. 2017. Disponível em: <https://freenetproject.org/pages/about.html>. Acesso em: 16 nov. 2017.

FOCAULT, 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 take-down: Another 413 illicit services based on the Tor network were closed in an international crackdown on online drugs trade. **The Guardian.** London, p. 1-5. 07 nov. 2014.

FOX-BREWSTER, Tom. Facebook opens up to anonymous Tor users with .onion address: Warns of 'evolutionary and flaky nature' of experiment to ensure anonymous users aren't wrongly identified as botnets. **The Guardian.** London, p. 1-3. 31 out. 2014. Disponível em: <https://www.theguardian.com/technology/2014/oct/31/facebook-anonymous-tor-users-onion>. Acesso em: 25 fev. 2018.

GARDNER, Joshua. Anonymous online marketplace that replaced Silk Road VANISHES... taking $100MILLION of users' money with it. **Daily Mail.** London, p. 1-6. 03 dez. 2013. Disponível em:

<http://www.dailymail.co.uk/news/article-2517244/Illegal-online-marketplace-replaced-Silk-Road-VANISHES--taking-100MILLION-users-money-it.html>. Acesso em: 25 fev. 2018.

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 out. 2014. SAGE Publications. http://dx.doi.org/10.1177/1461444814554900.

GHAPPOUR, Ahmed. Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web. **Stanford Law Review.** Stanford, p. 1075-1136. abr. 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 ago. 2015. Informa UK Limited. http://dx.doi.org/10.1080/00918369.2015.1088316.

HALLONSTEN, Olof. The Politics of European Collaboration in Big Science. **Global Power Shift,** [s.l.], p.31-46, 2014. Springer Berlin Heidelberg. http://dx.doi.org/10.1007/978-3-642-55010-2_3.

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, abr. 2007.

HENDEL, Charles W.. **David Humes 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. Disponível em:

<https://www.theguardian.com/technology/2014/jul/25/new-ransomware-employs-tor-onion-malware>. Acesso em: 25 fev. 2018.

HERN, Alex. US Defence Department funded Carnegie Mellon research to break Tor. **The Guardian.** London, p. 1-2. 25 fev. 2016. Disponível em: <https://www.theguardian.com/technology/2016/feb/25/us-defence-department-funding-carnegie-mellon-research-break-tor>. Acesso em: 25 fev. 2018.

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.i.], v. 24, n. 4, p.635-638, out. 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 fev. 2010. Association for Computing Machinery (ACM). http://dx.doi.org/10.1145/1698750.1698753.

HORSMAN, Graeme. Can we continue to effectively police digital crime? **Science & Justice**, [s.l.], v. 57, n. 6, p.448-454, nov. 2017. Elsevier BV. http://dx.doi.org/10.1016/j.scijus.2017.06.001.

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, fev. 2013. Informa UK Limited. http://dx.doi.org/10.1080/01402390.2012.739561.

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. IEEE. http://dx.doi.org/10.1109/isi.2012.6284146.

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 set. 2007. p. 1-2. Disponível em: <http://www.washingtonpost.com/wp-dyn/content/article/2007/09/10/AR2007091001192.html>. Acesso em: 24 fev. 2018.

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. University of Chicago Press. http://dx.doi.org/10.1086/507133.

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 State. **First Monday,** [s.l.], v. 17, n. 7,

p.1-17, 2 jul. 2012. University of Illinois Libraries. **http://dx.doi.org/10.5210/fm.v17i7.3848**.

LEE, Micah. **Edward Snowden explains how to reclaim your privacy**. 2015. Disponível em: <https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy/>. Acesso em: 07 dez. 2016.

LI, Bingdong et al. An Analysis of Anonymizer Technology Usage. **Traffic Monitoring And Analysis**, [s.l.], p.108-121, 2011. Springer Berlin Heidelberg. http://dx.doi.org/10.1007/978-3-642-20305-3_10.

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. Springer Berlin Heidelberg. http://dx.doi.org/10.1007/978-3-642-14992-4_19.

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 out. 2015. Informa UK Limited. http://dx.doi.org/10.1080/1369118x.2015.1093531.

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. Oxford University Press (OUP). http://dx.doi.org/10.1111/j.1468-2478.2010.00592.x.

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 out. 2013. SAGE Publications. http://dx.doi.org/10.1177/1748895813505234.

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. IOS Press. http://dx.doi.org/10.3233/thc-161244.

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 Yotk: 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. Disponível em: <http://journal.georgetown.edu/wp-content/uploads/2015/07/gj127_Cyber_Issue_2012.pdf>. Acesso em: 12 nov. 2017.

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 Obsfucation 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, abr. 2013.

MOORE, Daniel; RID, Thomas. Cryptopolitik and the Darknet. **Survival,** [s.l.], v. 58, n. 1, p.7-38, 2 jan. 2016. Informa UK Limited. http://dx.doi.org/10.1080/00396338.2016.1142085.

MORGENTHAU, Hans J.. **Politics Among Nations: T**he 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, abr. 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. Disponível em: <https://www.washingtonpost.com/news/morning-mix/wp/2014/11/04/with-tor-facebook-is-first-giant-social-media-outlet-to-venture-into-the-dark-web/?utm_term=.54314b151409>. Acesso em: 25 fev. 2018.

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. Oxford University Press (OUP). http://dx.doi.org/10.1111/misr.12024.

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 Security1. **Ethics And Information Technology,** [s.l.], v. 7, n. 2, p.61-73, jun. 2005. Springer Nature. http://dx.doi.org/10.1007/s10676-005-4582-3.

NYE, Joseph S.. **Cyber Power.** Cambridge: Belfer Center For Science And International Affairs, 2010. 24 p. Disponível em:<http://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf>. Acesso em: 09 set. 2017.

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. Disponível em: <http://www.belfercenter.org/sites/default/files/files/publication/global-cyber-final-web.pdf>. Acesso em: 3 set. 2017.

PACE, Jonathan. Exchange relations on the dark web. **Critical Studies In Media Communication,** [s.l.], v. 34, n. 1, p.1-13, 17 out. 2016. Informa UK Limited. http://dx.doi.org/10.1080/15295036.2016.1243249.

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. Informa UK Limited. http://dx.doi.org/10.1080/14702436.2011.590046.

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. IEEE. http://dx.doi.org/10.1109/ares.2008.63.

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, abr. 2018. Elsevier BV. http://dx.doi.org/10.1016/j.drugpo.2018.01.003.

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 ago. 2013. Disponível em: <https://www.washingtonpost.com/news/the-switch/?p=886&utm_term=.a13c54a98420>. Acesso em: 25 fev. 2018.

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, dez. 2014. Elsevier BV. http://dx.doi.org/10.1016/j.diin.2014.08.001.

PILKINGTON, Ed. Chelsea Manning released from military prison: American army private is free after serving seven years of 35-year sentence for leaking classified documents and videos downloaded to WikiLeaks. **The Guardian.** London, p. 1-3. 17 maio 2017. Disponível em: <American army private is free after serving seven years of 35-year sentence for leaking classified documents and videos downloaded to WikiLeaks>. Acesso em: 17 mar. 2018.

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 maio 2014. Disponível em: <https://www.theguardian.com/technology/2014/may/30/life-after-silk-road-how-the-darknet-drugs-market-is-booming>. Acesso em: 25 fev. 2018.

PRIGG, Mark; PRESS, Associated. 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. **Daily Mail.** London, p. 1-6. 06 nov. 2014. Disponível em: <http://www.dailymail.co.uk/sciencetech/article-2823926/Feds-Silk-Road-sequel-leads-California-arrest.html>. Acesso em: 25 fev. 2018.

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 abr. 2016. Informa UK Limited. http://dx.doi.org/10.1080/1097198x.2016.1172952.

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. Elsevier BV. http://dx.doi.org/10.1016/j.orbis.2014.02.009.

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. Brill Academic Publishers. http://dx.doi.org/10.1163/187119111x590556.

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. Informa UK Limited. http://dx.doi.org/10.1080/10282580.2013.798694.

RUSHE, Dominic. Silk Road 2.0's alleged owner arrested as drugs website shuttered by FBI: Blake Benthall, 26, arrested after allegedly resurrected drugs and contraband goods market after original incarnation was shut down by the FBI last year. **The Guardian.** London, p. 1-5. 06 nov. 2014. Disponível em: <https://www.theguardian.com/technology/2014/nov/06/silk-road-20-owner-arrested-drugs-website-fbi>. Acesso em: 25 fev. 2018.

SANDVIK, Runa. **The New York Times is Now Available as a Tor Onion Service**. 2017. Disponível em: <https://open.nytimes.com/https-open-nytimes-com-the-new-york-times-as-a-tor-onion-service-e0d0b67b7482>. Acesso em: 5 dez. 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. Cap. 1. p. 3-28.

SCHNEIDER, Jacquelyn. **Digitally-enabled Warfare:** the Capability-Vulnerability Paradox. 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. Cogitatio. http://dx.doi.org/10.17645/mac.v5i1.805.

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. **Anais... .** 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 TERMSa. **The Tech Terms Computer Dictionary**. 2017. Disponível em: <https://techterms.com/definition/script>. Acesso em: 02 dez. 2017.

TECH TERMSb. **The Tech Terms Computer Dictionary**. 2017. Disponível em: <https://techterms.com/definition/relational_database>. Acesso em: 02 dez. 2017.

THOMSON, Iain. **Dark web doesn't exist, says Tor's Dingledine. And folks use network for privacy, not crime:Cofounder brings us up to**

date on network status. 2017. Disponível em: <https://www.theregister.co.uk/2017/07/29/tor_dark_web/>. Acesso em: 29 out. 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. Disponível em: <http://journal.georgetown.edu/wp-content/uploads/2015/07/gj127_Cyber_Issue_2012.pdf>. Acesso em: 12 nov. 2017.

TOR PROJECT. **Projects**. Disponível em: <https://www.torproject.org/projects/projects.html.en>. Acesso em 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. Elsevier BV. http://dx.doi.org/10.1016/j.drugpo.2018.01.022.

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. Springer Nature. http://dx.doi.org/10.1007/s10669-013-9480-3.

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. Elsevier BV. http://dx.doi.org/10.1016/j.drugpo.2013.10.009.

VITALIEV, Dmitri. Vaulting the great Firewall. **The Guardian.** London, p. 1-2. 05 ago. 2008. Disponível em: <https://www.theguardian.com/commentisfree/2008/aug/05/china.censorship>. Acesso em: 25 fev. 2018.

WALSH, Lucas; BARBARA, Julien. Speed, International Security, and. **Journal Of Computer-mediated Communication,** [s.l.], v. 12, n. 1, p.189-208, out. 2006. Wiley-Blackwell. http://dx.doi.org/10.1111/j.1083-6101.2006.00321.x.

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.i.], 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, ago. 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 (Org.). **Featured.** 2016. Disponível em: <https://wikileaks.org/>. Acesso em: 08 set. 2016.

WRIGHT, Quincy. **The study of International Relations.** Nova York: Appleton-century-crofts, 1955.

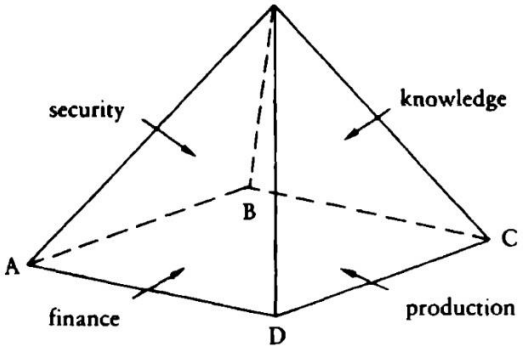
WRIGHT, Quincy. **A Study of War:** Volume I. Chicago: Chigago Press University, 1942.

WRIGHT, Quincy. **A Study of War:** Volume II. Chicago: Chigago Press University, 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, set. 2016. IEEE. http://dx.doi.org/10.1109/isi.2016.7745452.

ANEXO

ANEXO 1 – PIRÂMIDE REPRESENTATIVA DO PODER ESTRUTURAL



Fonte: STRANGE, 1988, p.27

ANEXO 2 – DIMENSÕES FÍSICAS E VIRTUAIS DO PODER CIBERNÉTICO

Table 1: Physical and Virtual Dimensions of Cyber Power

	Targets of Cyber Power: Intra cyber space	Targets of Cyber Power: 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

Fonte: NYE, 2010, p.5

ANEXO 3 – REDE DISTRIBUTIVA

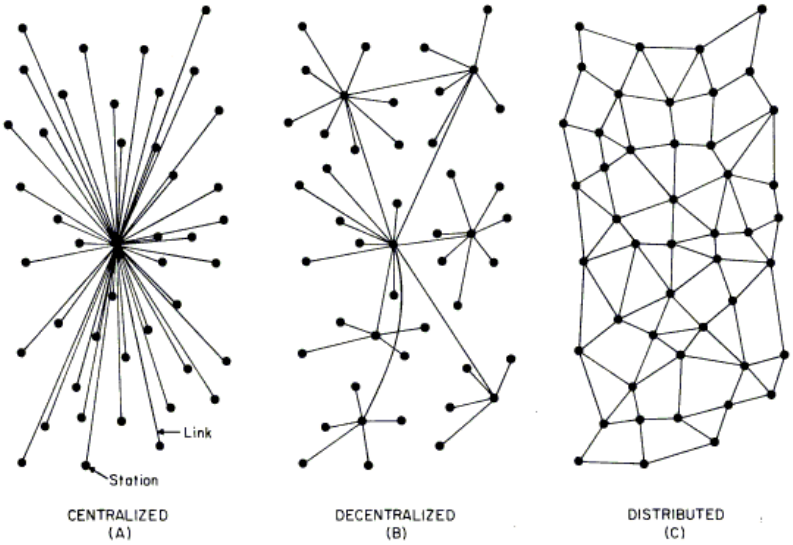


FIG. 1 — Centralized, Decentralized and Distributed Networks

Fonte: BARAN, 1964, p.2

ANEXO 4 – VOLUME TRÁFEGO DE DADOS POR PROTOCOLO NO "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

Fonte: NAUGHTON, 1999, p.248

ANEXO 5 – AS VÁRIAS WEBS

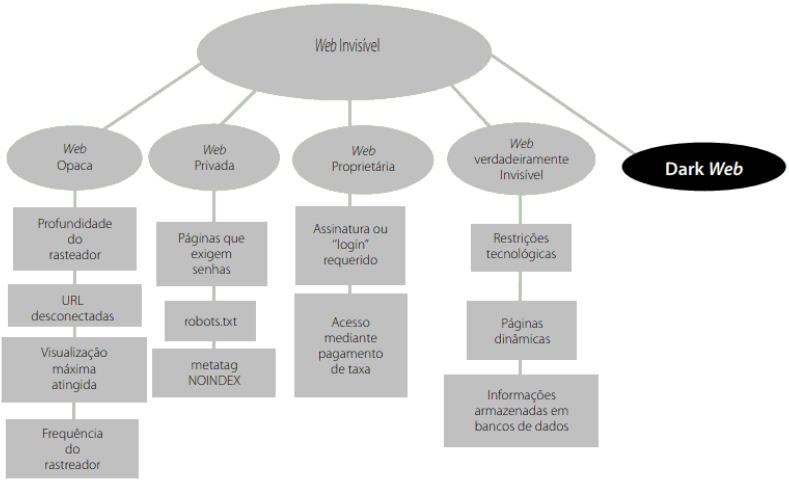
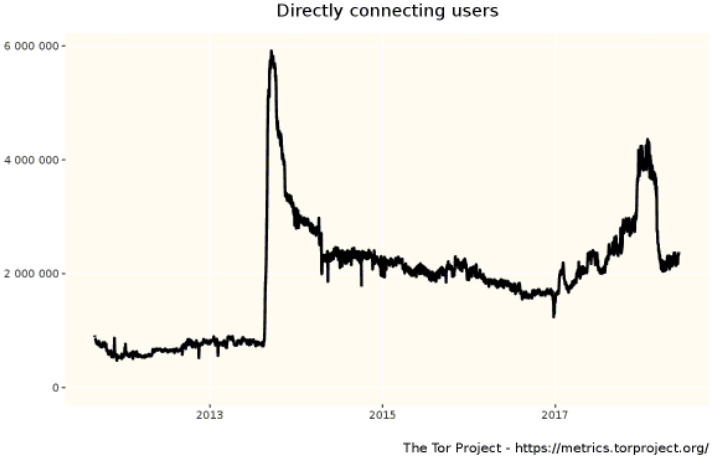


Figura 2. As várias *Web*.

Fonte: FIDÊNCIO; MONTEIRO, 2013, p.41

ANEXO 6 - "DIRECTLY CONNECTING USERS"



Fonte: THE TOR PROJECT, 2018 (metrics.torproject.org)

ANEXO 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

Fonte: MOORE; RID, 2016. p.21

APÊNDICE

APÊNDICE 1 – SER AUTORIDADE

TRECHOS DA OBRA "THE RETREAT OF THE STATE: THE DIFFUSION OF POWER IN THE WORLD ECONOMY", DE SUSAN STRANGE, 1996

Página	"TO BE AN AUTHORITY"
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.
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.168	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.
p.171	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.
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.

Fonte: STRANGE, 1996.

APÊNDICE 2 – EXERCER AUTORIDADE

TRECHOS DA OBRA "THE RETREAT OF THE STATE: THE DIFFUSION OF POWER IN THE WORLD ECONOMY", DE SUSAN STRANGE, 1996

Página	"TO EXERCISE AUTHORITY"
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.
p.197	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.
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.

Fonte: STRANGE, 1996.

APÊNDICE 3 – CONTROLE, 1988

TRECHOS SOBRE CONTROLE EM "STATES AND MARKETS", de Susan Strange, 1988		
Página	**CITAÇÃO**	**OBJETO**
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
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. 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 oilwells, 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.	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 lndia. Trade deficits elsewhere in the world economy were matched by a persistent trade surplus from 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

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. The belief in resurrection after death was strong enough and pervasive enough for legitimate power to be conferred upon those in the Church or the great religious orders whose claims to possession of this knowledge were generally acknowledged. Since the expectation of life in those days was so brief, and the knowledge of how to improve the conditions of aterial life and to guard against the hazards to the body of famine, plague and violence was so scanty, the alternative religious knowledge concerning the remission of sins and the acquisition of external salvation for the soul was highly valued. From this, and not in the last resort from military might or material wealth, the princes of the Church and their underlings drived power and authority over the laity. 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. The price of such dependence must be some increased susceptibility to corporate influence in policy-making, especially in Washington.	Systems reserved to the Pentagon
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	Airspace / territorial waters
p.188	The United States has dominated and directed the negotiations in the GAIT, for example initiating the Multifibre Agreement negotiations and first blocking and then accepting under limits the GSP. It has been able to do so partly because of its implicit bargain with its NATO/OECD allies that gave it a free hand in monetary management and trade negotiations in return for a nuclear defence umbrella; and 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. By that time, oil had taken the place of coal as the object of national strategy and international diplomacy. Energy was still 'high politics' - but energy came from a different source. And until the North Sea oilfields were developed, 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 - using a political event to jack up prices. But the second oil price rise was quite soon defeated, not by other governments but by the market. By March 1983, 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. Prices fell still more, despite the cutbacks self-imposed by Saudi Arabia and agreed by other OPEC states. The fourth phase of state domination was definitely over.	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	An alternative view, to which I hold and which I believe is held by a too-silent majority of non-American scholars - in Russia and the former socialist countries, Europe, Japan, Canada and the Third World - disagrees with both the American liberals and the American realists on the causes of world economic disorder, but is probably closer to the realists when it comes to remedies. The disagreement on causes is that 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. But the structural power it has acquired in recent decades has been misused in the service of narrow national interests. While this misuse of power has sheltered the US taxpayer and consumer (and to a lesser extent, workers) in the short run, it runs a serious risk in the long run of weakening both the system and the structural hegemony of the United States.	Structures of the world system
p.242	True, that when President Bush decided to contest the Iraqi invasion of Kuwait in 1990, there was a brief period when the US worked hard to gain the support of other states in the UN Security Council. But once assured of a UN blessing, 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

Fonte: STRANGE, 1988.

APÊNDICE 4 – CONTROLE, 1996

TRECHOS SOBRE CONTROLE EM "THE RETREAT OF THE STATE: DIFFUSION OF POWER IN THE WORLD ECONOMY", de Susan Strange, 1996

Página	CITAÇÃO	OBJETO
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
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 [post, telegraph, telefone] used to have control over the design and availability of such communications. No longer. The prospect in the mid-1990s is for a mere handful of global corporations to take the place of many mostly publicly owned national operators, and to dominate the business world-wide. Governments everywhere are being forced, willynilly, to bargain with these transnational operating firms over the terms on which national systems are incorporated into the global network and the ways in which they develop. […] 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. The story also underlines the power of markets over states.	Post, telegraph and telephone [PTTs] / design, availability of the PPTs 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. The efforts of states, individually and collectively, to use their countervailing powers in the interest of society as a whole and including the weak and the poor seem to have failed, at least for the time being.	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 (see La Repubblica, 28 January 1995).	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 – the responsibility for maintaining law and order and administering criminal justice. It would require a worldwide police authority – and not just the proposed Europol - with extensive powers to arrest and prosecute the criminals anywhere in the world, including the United States. It would probably require giving governments the power to confiscate or sequester any properties or funds judged to have been acquired through illegal trading. It would also require an international court of criminal justice able to judge and punish. This is something that, so far, no government of a nation-state has ever contemplated. 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
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. Some private protectionism is legitimised by governments as with pharmaceutical patents, or public procurement policies that discriminate in favour of a particular protected firm to the exclusion of others.	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. The supporting role of the South African, Soviet and Israeli governments was just that – supportive.	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. At the time of writing, the shift to Brussels affects only the trivial pursuits of an international bureaucracy. 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
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

Fonte: STRANGE, 1996.

APÊNDICE 5 – ARTIGOS PUBLICADOS EM 2013

TABELA 5 - Nº ARTIGOS PUBLICADOS POR ASSUNTO EM 2013

Assunto	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**

Fonte: Autora.

APÊNDICE 6 – ARTIGOS PUBLICADOS EM 2014

TABELA 6 - Nº ARTIGOS PUBLICADOS POR ASSUNTO EM 2014

Assunto	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**

Fonte: Autora.

APÊNDICE 7 – ARTIGOS PUBLICADOS EM 2017

TABELA 7 - Nº ARTIGOS PUBLICADOS POR ASSUNTO EM 2017

Ator	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**

Fonte: Autora.

APÊNDICE 8 – ARTIGOS E OCORRÊNCIAS PARA ANÁLISE POR ANO

TABELA 8 - Nº DE ARTIGOS ANALISADOS E Nº DE OCORRÊNCIAS TOTAL PARA ANÁLISE (2007-2017)

Ano	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**

Fonte: Autora.

*Analisados (A); Ocorrências (O); Repetidos (R)

APÊNDICE 9 – ANÁLISE DE DIFUSÃO POR ATOR E GRUPO

TABELA 9 - GRUPOS E ATORES: NÚMERO DE OCORRÊNCIAS (N) POR DIMENSÃO ATRAVÉS DE PUBLICAÇÕES JORNALÍSTICAS (2007-2017)

			AUTORIDADE			CONTROLE			RESULTADO	
GRUPO TEMÁTICO	ATOR	OCORRÊNCIAS	Decrescimento	Estabilidade	Crescimento	Nenhum	Parcial	Absoluto	Não-alteração	Alteração
		N	N	N	N	N	N	N	N	N
Surveillance Circunvention		**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
	Sheep Marketplace	**1**	1	0	0	0	0	1	1	0
Privacy		**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**
	Doxbin		0	1	0	0	1	0	1	0
Total		**139**	**57**	**29**	**53**	**2**	**55**	**82**	**62**	**77**

Fonte: Autora.

LINE	COUNTRY	NEWSPAPER	ARTICLE TITLE	AUTHOR	YEAR	ACTOR	CATEGORY	PEERS	AUTHORITY	OBJECT	CONTROL	STATUS QUO	OUTCOMES	EFFECT ON REALITY	REPEATED ARTICLES
1	USA	The Washington Post	"Researcher intercepted embassy passwords"	Jeremy Kirk	set/07	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	ago/08	Tor Project	Surveillance Circunvention	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	ago/08	Tor Project	Surveillance Circunvention	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	dez/09	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	jul/09	Tor Project	Surveillance Circunvention	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	dez/10	Wikileaks	Journalism & Whistleblowing	Governments, journalists, worlwide citizens, activists	1	Storage of information	0	Government Privacy	1	YES	NO

7	USA	The NY Times	"Granting Anonymity"	Virginia Heffernan	dez/10	Tor Project	Surveillance Circunvention	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	nov/11	Tor Project	Surveillance Circunvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	No donation of bandwidth to the **Tor Network** (virtual)	0	NO	NO
9	UK	The Telegraph	"Iran cracks down on web dissident technology"	Christopher Williams	mar/11	Tor Project	Surveillance Circunvention	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	MLIV E.com	"Coldwater man among 15 arrests in international online drug probe"	The Associated Press	abr/12	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	abr/12	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	ago/13	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	out/13	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	out/13	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	nov/13	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	out/13	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"	James Ball, Charles Arthur and Adam Gabatt	out/13	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 Guardian	"Filesharing search engines take to dark web and Bitcoin to escape Hollywood"	Samuel Gibbs	nov/13	Tor Project	Surveillance Circunvention	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	jun/13	Tor Project	Surveillance Circunvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	Steady number of users	0	NO	NO
20	UK	The Guardian	"How a Russian cybercriminal tried to frame me with a Bitcoin heroin deal"	Brian Krebs	jul/13	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's Silk Road was working with FBI for months before huge bust"	Daily Mail Reporter	out/13	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	Daily Mail	"Anonymous online marketplace that replaced Silk Road VANISHES... Taking $100MILLION of users' money with it"	Joshua Gardner	dez/13	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	set/13	Tor Project	Surveillance Circunvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	To not keep your 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	ago/13	Tor Project	Surveillance Circunvention	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	nov/13	Tor Project	Surveillance Circunvention	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, cocaine, even hitmen for hire are a few clicks away on the internet"	Steve Boggan	nov/13	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	out/13	Tor Project	Surveillance Circunvention	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 opens"	Reuters (edited by Bonnie Malkin)	nov/13	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	out/13	Edward Snowden	Journalism & Whistleblowing	Governments, private citizens, journalists, activists, dissidents	1	Information on NSA surveillance, including on Tor Network (with documents)	1	No actionsn specifically targeting NSA	0	NO	NO

30	UK	The Guardian	"NSA Files: Decoded; Caught in a Net"	Nadja Popovich and Greg Chen	nov/13	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 unaware and not taking action	1	YES	NO
31	UK	The Guardian	"NSA Files: Decoded; Pretty Good Privacy"	Greg Chen and Gabriel Dance	nov/13	Tor Project	Surveillance Circunvention	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	jan/14	Tor Project	Surveillance Circunvention	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	nov/13	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	set/13	Tor Project	Surveillance Circunvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	No actions by the NSA	1	YES	NO
35	UK	Daily Mail	"Man accused of operating notorious online drugs market Silk Road (and earning $80 million in commission) ordered to New York to face charges"	Associated Press	out/13	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	out/13	Tor Project	Surveillance Circunvention	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 documents show campaign against Tor encrypted network"	Barton Gellman, Craig Timberg and Steven Rich	out/13	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	out/13	Silk Road	Online Marketplace	Private citizens	-1	Marketplace Site and its payment mechanism	2	-	0	NO	NO
39	UK	Daily Mail	"Man behind Silk Road drug gang 'planned to carry out six murders' "	Shari Miller	nov/13	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
40	UK	The Guardian	"Silk Road underground market closed but others will replace it"	Samuel Gibbs	out/13	Silk Road	Online Marketplace	Private citizens	0	Marketplace Site and its payment mechanism	2	-	0	NO	YES
41	UK	The Guardian	"Silk Road underground market closed but others will replace it"	Samuel Gibbs	out/13	Tor Project	Surveillance Circunvention	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	mar/14	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 salvo in the 'war between data capture and privacy'"	Ed Pilkington	mai/13	Wikileaks	Journalism & Whistleblowing	Private citizens, dissidents, journalists, activists, state governments	0	Storage of information	1	No discussion on NSA, US government actions, worldwide state governments	1	YES	YES
44	UK	The Guardian	"Strongbox: New Yorker's salvo in the 'war between data capture and privacy'"	Ed Pilkington	mai/13	Strongbox	Journalism & Whistleblowing	Private citizens, dissidents, journalists, activists, state governments	1	Channel of communication and its storage (software)	1	-	0	NO	YES
45	UK	The Guardian	"Strongbox: New Yorker's salvo in the 'war between data capture and privacy'"	Ed Pilkington	mai/13	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	out/13	Tor Project	Surveillance Circunvention	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	dez/13	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	dez/13	Silk Road	Online Marketplace	Private citizens	-1	Marketplace Site and its payment mechanism	2	-	0	NO	NO
49	USA	The Washington Post	"The feds pay for 60 percent of Tor's development. Can users trust it?"	Brian Fung	set/13	Tor Project	Surveillance Circunvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists,	0	Tor Network	2	-	0	NO	NO

								state governments						
50	UK	The Guardian	"Tor: 'The king of high-secure, low-latency anonymity' "	The Guardian	out/13	Tor Project	Surveillance Circunvention	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	ago/13	Tor Project	Surveillance Circunvention	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	nov/13	Tor Project	Surveillance Circunvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	Parliament not discusing cybertools and privacy	1	YES	NO
53	USA	NOL A.com	"17 arrested in worldwide drug website bust; Silk Road 2.0 shut down"	The Associated Press	nov/14	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	dez/14	Tor Project	Surveillance Circunvention	Technical experts, private citizens, journalists, dissidents, military, human rights	-1	Tor Network	2	-	0	NO	NO

								groups, activists, state governments							
55	USA	OREGONLIVE.com	"'Dark net' investigation cracks down on Silk Road 2.0; 17 arrested"	The Associated Press	nov/14	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"	Associated Press	nov/14	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	nov/14	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	set/14	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	nov/14	Silk Road 2.0	Online Marketplace	Private citizens	-1	Marketplace Site	1	-	0	YES	YES

60	UK	Daily Mail	"Europol: 17 arrests in worldwide drug website bust"	The Associated Press	nov/14	Silk Road 2.0	Online Marketplace	Private citizens	-1	Marketplace Site	1	-	0	YES	NO
61	UK	The Guardian	"Evidence implicates governmentbacked hackers in Tor malware attacks"	Tom Fox-Brewster	nov/14	Tor Project	Surveillance Circunvention	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	out/14	Facebook	Surveillance Circunvention	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	nov/14	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	jul/14	Edward Snowden	Journalism & Whistleblowing	Governments, private citizens, journalists, activists, dissidents	1	Information on NSA surveillance, including on Tor Network (with documents)	1	No lawmakers beggining 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	abr/14	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	jun/14	SecureDrop System	Journalism & Whistleblowing	Private citizens, dissidents, journalists, activists, state governments	1	Channel of communication and its storage (software)	1	-	0	NO	YES
67	UK	The Guardian	"Guardian launches SecureDrop system for whistleblowers to share files"	James Ball	jun/14	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	nov/14	Silk Road 2.0	Online Marketplace	Private citizens	-1	Marketplace Site	1	No trade of illegal products	1		NO
69	UK	The Guardian	"Life after Silk Road: how the darknet drugs market is booming"	Mike Power	mai/14	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	jul/14	Onion ransomware	Digital Security	Private citizens, dissidents, journalists, activists, state governments	1	Channel of information 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	nov/14	Tor Project	Surveillance Circunvention	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 the Tor Network	1	YES	YES
72	UK	The Guardian	"Operation Onymous may have exposed flaws in Tor, developers reveal"	Alex Hern	nov/14	Silk Road 2.0	Online Marketplace	Private citizens	-1	Marketplace Site	1	-	0	NO	NO
73	UK	The Guardian	"Researchers: Lawyers blocked our Black hat demo on de anonymising Tor"	Tom Brewster	jul/14	Tor Project	Surveillance Circunvention	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 roubles for 'research to identify users of Tor'"	Alec Luhn	jul/14	Tor Project	Surveillance Circunvention	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	nov/14	Silk Road 2.0	Online Marketplace	Private citizens	-1	Marketplace Site	1	No trade of illegal products	1	YES	NO
76	UK	The Guardian	"Silk Road 2.0 targeted in 'Operation Onymous' darkweb takedown"	Tom Fox-Brewster	nov/14	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	nov/14	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	nov/14	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 Reporter	fev/14	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"	Associated Press and Mark Prigg	nov/14	Silk Road 2.0	Online Marketplace	Private citizens	-1	Marketplace Site	1	No trade of illegal products	1	YES	NO
81	UK	The Guardian	"Simplocker Android malware locks up mobile data and demands a ransom"	Tom Brewster	jun/14	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 'Xnet' corruption fighters expose graft"	Associated Press	dez/14	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 'Xnet' corruption fighters expose graft "	Associated Press	dez/14	Wikileaks	Journalism & Whistleblowing	Governments, private citizens, journalists, activists, dissidents	1	Channel of communication and its storage (software)	1	Not inspiring similar actions in local communities	1	YES	YES
84	UK	Daily Mail	"Spain's 'Xnet' corruption ighters expose graft "	Associated Press	dez/14	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
85	UK	The Guardian	“The darkweb's nihilistic vigilante sees the light”	Tom Fox-Brewster	dez/14	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	dez/14	Tor Project	Surveillance Circunvention	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	nov/14	Tor Project	Surveillance Circunvention	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	jul/14	Tor Project	Surveillance Circunvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	-1	Tor Network	2	-	0	NO	NO
89	USA	The Washington Post	“The Switchboard: ‘Spoiled onions’ on the Tor network”	Andrea Peterson	jan/14	Tor Project	Surveillance Circunvention	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	out/14	Tor Project	Surveillance Circunvention	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	jul/14	Tor Project	Surveillance Circunvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists,	0	Tor Network	2	No public speeches on Tor Network	1	YES	NO

								state governments						
92	UK	The Guardian	"Tor may be forced to cut back capacity after Heartbleed bug"	Alex Hern	abr/14	Tor Project	Surveillance Circunvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	-	0	NO	NO
93	USA	The Washington Post	"Why was the Black Hat talk on Tor de-anonymization mysteriously canceled?"	Andrea Peterson	jul/14	Tor Project	Surveillance Circunvention	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 Ellen Nakashima	nov/14	Silk Road 2.0	Online Marketplace	Private citizens	-1	Marketplace Site	1	-	0	NO	YES
95	USA	The Washington Post	"U.S., European authorities strike against Internet's black markets"	Craig Timberg and Ellen Nakashima	nov/14	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	nov/14	Tor Project	Surveillance Circunvention	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	jul/14	Tor Project	Surveillance Circunvention	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 irst to use the Onion Router to allow anonymous browsing"	Richard Gray	jan/15	Tor Project	Surveillance Circunvention	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 Wm. Moyer	nov/14	Facebook	Surveillance Circunvention	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	set/14	Tor Project	Surveillance Circunvention	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	jan/15	Silk Road	Online Marketplace	Private citizens	-1	Marketplace Site and its payment mechanism	2	No courtroom decisions and judgments of private citizens over use of Tor or online marketplaces	1	YES	NO
102	USA	PENN LIVE. COM	"From Penn State student to Dread Pirate Roberts: Tale of the Silk Road drug kingpin"	Nick Malawskey	fev/15	Silk Road	Online Marketplace	Private citizens	-1	Marketplace Site and its payment mechanism	2	No courtroom decisions and judgments of private citizens over use of Tor or online marketplaces	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	nov/15	Tor Project	Surveillance Circunvention	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	out/15	Tor Project	Surveillance Circunvention	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	dez/15	Tor Project	Surveillance Circunvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	Kremlim 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	mai/15	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 ecstasy, cannabis and LSD to students on hidden 'Dark Web' internet site"	Euan McLelland	ago/15	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
108	INDIA	The Tribune	"Private data, public life"	Anurag Chakraborty	jul/15	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	jul/15	Tor Project	Surveillance Circunvention	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	fev/15	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	mai/15	Silk Road	Online Marketplace	Private citizens	-1	Marketplace Site and its payment mechanism	2	No huge revenues from drug sales on Online Marketplaces	1	YES	NO
112	UK	The Guardian	“Silk Road founder: 'it ruined my life and destroyed my future"'	Nicky Woolf	jan/15	Silk Road	Online Marketplace	Private citizens	-1	Marketplace Site and its payment mechanism	2	No drugs being trade over an online marketplace	1	YES	NO
113	UK	Daily Mail	“Silk Road mastermind Russ Ulbricht sentenced to life in jail for creating worldwide criminal enterprise that sold more than $200 million worth of drugs”	Reuters and Associated Press	mai/15	Silk Road	Online Marketplace	Private citizens	-1	Marketplace Site and its payment mechanism	2	No drugs being trade over an online marketplace	1	YES	NO
114	UK	The Guardian	“Surveillance Q&A: what web data is affected and how to foil the snoopers”	Samuel Gibbs	nov/15	Tor Project	Surveillance Circunvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists,	1	Tor Network	2	-	0	NO	NO

state governments

115	USA	The NY Times	“Trial Over a Man’s Role in a Black Market Begins”	Benjamin Weiser	jan/15	Silk Road	Online Marketplace	Private citizens	-1	Marketplace Site and its payment mechanism	2	No drugs being trade over an online marketplace	1	YES	NO
116	UK	Daily Mail	“US marshals to auction 50,000 bitcoins worth $11million that were coniscated from convicted Silk Road mastermind”	Reuters	fev/15	Silk Road	Online Marketplace	Private citizens	-1	Marketplace Site and its payment mechanism	2	No drugs being trade over an online marketplace	1	YES	NO
117	UK	Daily Mail	“US Marshals to auction dark web drug dealer's $11million bitcoin fortune: Bidders get the chance to buy Silk Road founder Ross Ulbricht's fortune... at a discount”	Darren Boyle	out/15	Silk Road	Online Marketplace	Private citizens	-1	Marketplace Site and its payment mechanism	2	No drugs being trade over an online marketplace	1	YES	NO
118	USA	The Washington Post	“Why ‘Dark Web’ drug markets will keep on imploding”	Henry Farrell	mar/15	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”	Associated Press	jun/15	Tor Project	Surveillance Circunvention	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	jan/16	Facebook	Surveillance Circunvention	Private citizens	1	Facebook Website through Tor Network	1	-	0	NO	NO
121	USA	PENNLIVE.COM	“Feds call former NSA contractor's theft of 50 terabytes of secrets 'breathtaking'”	Associated Press	out/16	Harold Martin (former NSA’s contractor)	Journalism & Whistleblowing	Private citizens, dissidents, journalists, activists, state governments	0	Documents from the NSA	1	-	0	NO	NO
122	UK	The Guardian	“How to contact the Guardian securely”	The Guardian	set/16	Tor Project	Surveillance Circunvention	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 for dark web”	Jasper Jackson	jan/16	ProPublica	Journalism & Whistleblowing	Private citizens, dissidents, journalists, activists, state governments	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	jan/16	Tor Project	Surveillance Circunvention	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 New Board”	Nicole Perlroth	jul/16	Tor Project	Surveillance Circunvention	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	fev/16	Carnegie Mellon University	Digital Security	Private citizens, dissidents, journalists, activists, state governments	1	Cybertools to attack the Tor Network	1	No FBI involvement in universities’ research on Tor Network, no courtrooms involved	1	YES	NO
127	UK	Daily Mail	“AlphaBay, the biggest illegal drugs marketplace in internet history, shut down by the Justice Department”	Hannah Parry	jul/17	Alphabay	Online Marketplace	Private citizens	-1	Marketplace Site	1	No drugs being trade 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	jul/17	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	jul/17	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	mar/17	Tor Project	Surveillance Circunvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	1	Tor Network	2	-	0	NO	NO

131	USA	OREGONLIVE.com	"'Dark web' marketplace AlphaBay shut down by feds"	The Washington Post	jul/17	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
132	UK	The Guardian	"Dark web marketplaces AlphaBay and Hansa shut down"	Samuel Gibbs and Lois Becket t	jul/17	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	jul/17	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 neoNazis and dissidents alike"	Alex Hern	ago/17	Tor Project	Surveillance Circunvention	Technical experts, private citizens, journalists, dissidents, military, human rights groups, activists, state governments	0	Tor Network	2	Not helping dissidents and voices around the globe	1	YES	NO

135	UK	Daily Mail	"US, European police say 'dark web' markets shut down"	AFP	jul/17	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	jul/17	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	jul/17	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	mai/17	Ransomware	Digital Security	Private citizens, dissidents, journalists, activists, state governments	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	dez/16	SecureDrop System	Journalism & Whistleblowing	Private citizens, dissidents, journalists, activists, state governments	1	Channel of communication and its storage (software)	1	-	0	NO	NO

FONTE:
Autora.