UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE GRADUAÇÃO
CURSO DE RELAÇÕES INTERNACIONAIS

ARTHUR MARTINI BRONZATTI

OS ATORES NÃO-ESTATAIS E ESTATAIS NO MUNDO CIBERNÉTICO E SUA INFLUÊNCIA NO SISTEMA INTERNACIONAL

Porto Alegre
2021

ARTHUR MARTINI BRONZATTI

OS ATORES NÃO-ESTATAIS E ESTATAIS NO MUNDO CIBERNÉTICO E SUA INFLUÊNCIA NO SISTEMA INTERNACIONAL

Projeto de Pesquisa apresentado como requisito parcial para obtenção do título de Bacharel em Relações Internacionais, pelo Curso de Relações Internacionais da Universidade do Vale do Rio dos Sinos – UNISINOS

Orientador: Prof. Dr. Marcos Aurélio Barbosa dos Reis

Porto Alegre

2021

ARTHUR BRONZATTI

OS ATORES NÃO-ESTATAIS E ESTATAIS NO MUNDO CIBERNÉTICO E SUA INFLUÊNCIA NO SISTEMA INTERNACIONAL

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Bacharel em Relações Internacionais, pelo Curso de Relações Internacionais da Universidade do Vale do Rio dos Sinos - UNISINOS

APROVADO EM: _____ / _____ / _____

BANCA EXAMINADORA

_____

Prof. Dr. Marcos Aurélio Barbosa dos Reis
Orientador - UNISINOS

_____

Profa. Dra. Nadia Barbacovi Menezes
Examinador Interno - UNISINOS

_____

Prof. Ms. Álvaro Augusto Stumpf Paes Leme
Examinador Interno - UNISINOS

AGRADECIMENTOS

Agradeço ao corpo de professores do curso de Relações Internacionais da UNISINOS por todo o conhecimento compartilhado e por toda a sabedoria que me foi entregue. Agradeço especialmente os professores Álvaro e Nadia, coordenadores do curso, por toda a atenção e suporte ao longo da graduação e por terem tornado a universidade uma experiência muito agradável.

Agradeço ao meu orientador, Marcos Reis, pelo apoio durante todo o desenvolvimento deste trabalho. Sem sua ajuda, esta pesquisa não teria sido possível.

Agradeço também a minha família, meus pais, Reges e Graziele, e meu irmão, Guilherme, por todo o auxílio e compreensão durante esta longa jornada. Seu amor e carinho foi muito importante para o meu sucesso.

Por fim, agradeço aos meus colegas e amigos da universidade que, ao meu lado, trilharam pelos mesmos desafios e adversidades. Obrigado, Alana, Alyssa, Ana Clara, Carmen, Dora, Fernanda, Henrique, Kethelin, Kevin, Lucas, Rafael e Tiago por todos os incríveis anos de amizade e companheirismo. O carinho de vocês foi meu suporte nos momentos mais difíceis.

RESUMO

São escassos os trabalhos que, dentro da disciplina de Relações Internacionais (RI), refletem sobre os efeitos do desenvolvimento do ciberespaço e de novas tecnologias digitais sobre o Sistema Internacional (SI), além de todos os elementos que o compõem. A falta de atenção atribuída a esse tema leva a uma desinformação generalizada, onde até mesmo acadêmicos consagrados acabam por desenvolver concepções errôneas ou até mesmo exageradas sobre o funcionamento do mundo cibernético, que, em última instância, leva os responsáveis pela criação de políticas públicas voltadas à regulação do domínio digital a tomarem decisões infundadas que apenas criam maiores problemas. A partir disso, o objetivo da presente monografia é explorar e discutir as principais características do ciberespaço, assim como refletir sobre como ele afeta a ação de Estados e atores não-estatais. O trabalho foi redigido através de uma metodologia exploratória de caráter descritiva, sendo possível concluir que, apesar de ser capaz de empoderar indivíduos e grupos minoritários, a utilização do ciberespaço sozinho por ativistas ou terroristas têm impacto insignificante no SI. Entretanto, a utilização do mundo virtual pode ser valiosa para aqueles Estados que possuírem o conhecimento e a capacidade para manipulá-lo de maneira inteligente — especialmente se usado para interferir em decisões políticas de diferentes nações.

Palavras-chaves: Ciberespaço. *Big Data*. Sistema Internacional. Teoria da Interdependência Complexa. Internet das Coisas.

ABSTRACT

There are few works, within the discipline of International Relations (IR), that reflect on the effects of the development of Cyberspace and new digital technologies on the International System and all the elements that compose it. The lack of attention given to this topic leads to widespread misinformation, where even established academics end up developing erroneous and exaggerated conceptions about the functioning of the cyber world, which ultimately leads those responsible for creating public policies aimed at regulating the digital domain to make unfounded decisions that only create greater problems. Based on this, the objective of this monograph is to explore and discuss the main characteristics of Cyberspace, as well as reflect on how it affects the actions of States and non-state actors. The work was written through an exploratory methodology of descriptive nature, and was able to conclude that, despite being able to empower individuals and minority groups, the use of Cyberspace alone by activists or terrorists has an insignificant impact on the International System. However, the use of the virtual world can be valuable to those states that possess the knowledge and ability to manipulate it intelligently, especially if used to interfere in the political decisions of different nations.

Keywords: Cyberspace. Big Data. International System. Complex Interdependence Theory. Internet of Things.

LISTA DE SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

BDI – *Behavioural Dynamics Institute*

CIA – Agência Central de Inteligência

CISA – Cybersecurity Information Sharing Act

CISPA – Cyber Intelligence Sharing and Protection Act

DARPA – Agência de Projetos e Pesquisas Avançadas do Departamento de Defesa dos Estados Unidos

DSEI – *Defense and Security Equipment International*

FBI – Escritório Federal de Investigação

FISA – *Foreign Intelligence Surveillance Act*

GIFT – Global Internet Freedom Task Force

GDPR – General Data Protection Regulation

HDX – Humanitarian Data Exchange

KGB – Comitê de Segurança do Estado

LGPD – Lei Geral de Proteção de Dados

LeT – Lashkar-e-Taiba

MIT – Massachusetts Institute of Technology

NSA – Administração Nacional de Segurança dos EUA

ONU – Nações Unidas

OPEP – Organização dos Países Exportadores de Petróleo

OSINT – inteligência de código aberto

OTAN – Organização do Tratado do Atlântico Norte (OTAN)

PCC – Partido Comunista da China

RFID – Identificação por radiofrequência

RI – Relações Internacionais

SCS – Sistema de Crédito Social (SCS)

SCL – *Strategic Communication Laboratories*

TIA – Total Information Awareness (TIA)

USB – Universal Serial Bus

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho tem como tema de pesquisa o papel que as novas tecnologias podem ter sobre as Relações Internacionais (RI) e o impacto que seu surgimento pode causar dentro da balança de poder mundial. Além disso, a monografia explora a forma com que os Estados utilizam do ciberespaço a seu favor, e como atores não-estatais podem utilizar desse mesmo ambiente para desafiar o poder estatal. Dentro deste escopo, procura-se responder a seguinte pergunta-problema: de que forma os atores estatais e não-estatais atuam no ciberespaço e influenciam o Sistema Internacional (SI) através dele?

Os avanços tecnológicos modernos trouxeram novas dinâmicas que grande parte dos autores clássicos de RI deixaram de prever para o SI. A revolução tecnológica do século XXI introduziu novas ferramentas digitais e novas dinâmicas sociais que romperam com métodos tradicionais de se fazer política. A sociedade agora tem de lidar com fenômenos inéditos como ciberterrorismo e *fake news*, e o crime e a violência agora não são mais limitados pelas dimensões físicas.

No mundo contemporâneo observa-se que o indivíduo conectado ao mundo virtual está exposto na internet para quem quiser tirar proveito. Tamanha falta de privacidade na sociedade moderna pode acarretar inconveniências como ligações indesejadas ou até mesmo clonagem de cartões de créditos. Entretanto, o fácil acesso a dados pessoais de bilhões de pessoas gera implicações maiores a um nível macro que inclui Estados e grandes organizações.

A partir de tais acontecimentos, os Estados podem utilizar da cibernética não somente para travar uma guerra, mas para vigiar sua população extensivamente e manipular suas opiniões. Da mesma forma, o fenômeno pode ser usado por atores não-estatais, sejam eles organizações terroristas ou empresas multinacionais, para atingir interesses privados.

Com base nisso, este trabalho tem como problema de pesquisa os efeitos trazidos pelos novos fenômenos dentro da área da tecnologia, tais quais o *Big Data*, a Internet das Coisas, e o ciberespaço de maneira geral. Essa pesquisa busca entender os novos modelos de interações entre Estados soberanos e entre Estados e atores não-estatais, sendo delimitada pela atuação desses atores no Ciberespaço contemporâneo.

Como objetivo geral, este trabalho busca verificar como os atores não-estatais e estatais utilizam das novas tecnologias, como *Big Data* e Internet das Coisas, no "ciberespaço contemporâneo" e sua influência no SI, além de explorar como isso poderia causar uma mudança na balança de poder mundial.

Os objetivos específicos deste trabalho incluem discutir os conceitos de ciberespaço, Internet das Coisas, *Big Data*, Interdependência Complexa e SI; explorar como o ciberespaço pode ser usado a favor de atores não-estatais para desafiar o poder dos estados, influenciando o SI; entender como Estados soberanos estão atuando no Ciberespaço e como isso tem influenciado o SI;

Devido à influência que o Ciberespaço possui sobre as RI, essa pesquisa se justifica por sua importância tanto no âmbito teórico quanto no âmbito pragmático; no primeiro, ocorre por sua importância como pesquisa complementar à corrente teórica de interdependência complexa, e, no âmbito prático, porque seu objeto de pesquisa pode possuir implicações globais. Assim, um estudo dessas novas tecnologias sobre um ponto de vista político pode ser necessário para a tomada de decisões futuras.

A presente pesquisa possui como paradigma metodológico o interpretativista, pois não considera a existência de uma realidade totalmente objetiva nem subjetiva, mas sim uma interação entre as características de um determinado objeto e entre a compreensão que os seres humanos criam a respeito desse objeto (SACCOL, 2009).

Desta forma, a monografia ocorre através das lentes interpretativistas — prevalecendo a lógica indutiva ao não serem impostos entendimentos prévios sobre a situação pesquisada, evitando, também, a imposição de categorias para o estudo empírico do fenômeno do ciberespaço e sua influência no cenário internacional (SACCOL, 2009).

Com relação à metodologia, essa pesquisa pode ser classificada como exploratória de caráter descritivo e se utilizará de uma abordagem qualitativa. A partir disso, esse trabalho possui o intuito de explorar o problema de pesquisa e fornecer informações para um estudo mais preciso, além de tentar estabelecer as bases que levarão a pesquisas futuras (DIANA, 2020).

O método a ser utilizado será o estudo de caso comparado. Tal metodologia foi escolhida por se adequar ao tipo de pesquisa em vigor, pois, para poder entender o fenômeno do ciberespaço e como ele funciona na realidade, não há maneira melhor do que a análise de casos concretos onde essa tecnologia foi aplicada. Devido ao fato de que o tema do trabalho é um tópico de estudo que ainda se encontra em sua

infância, é importante que essa pesquisa seja de caráter exploratório, pois poderá servir de referência a trabalhos futuros.

Como parte do primeiro capítulo, na introdução será apresentado, primeiramente, o problema de pesquisa discutido ao longo do trabalho e sua relevância para a área de RI. Após, será redigido um sumário detalhado sobre o corpo da monografia.

No segundo capítulo, como referencial teórico, serão descritos os conceitos-chave presentes no texto e que são necessários para a compreensão do tema, como o conceito de ciberespaço e *Big Data*, assim como os principais conceitos por detrás da Teoria de Interdependência Complexa, além da definição de SI.

Dentro do terceiro capítulo, será feita uma série de estudos de casos nos quais o ciberespaço foi utilizado por atores não-estatais de modo a alcançar objetivos políticos privados que, por sua vez, repercutiram em uma escala global. O objetivo do capítulo é demonstrar como os Estados tornam-se vulneráveis frente ao domínio cibernético.

No capítulo quarto, será analisado, através de uma série de estudos de casos variados, a forma como Estados utilizam-se do ciberespaço a seu favor. Será discutida, também, a veracidade de algumas alegações feitas com relação ao ciberespaço e as presunções de que ele possa subjugar o papel do Estado na Sociedade Internacional.

Para concluir o trabalho, será feito uma breve recapitulação dos pontos mais importantes debatidos durante o texto e dos resultados encontrados, respondendo à pergunta-problema. Mais importante, será feita uma breve reflexão que leve em consideração a importância da pesquisa e incentive a produção de projetos futuros sobre o tema.

Com relação à ética do mundo acadêmico, este estudo garante o cumprimento de todas as normas estabelecidas pela Associação Brasileira de Normas Técnicas (ABNT), incluindo o plágio.

2 MARCO TEÓRICO CONCEITUAL

Neste capítulo será apresentado o marco teórico conceitual que servirá como base fundamental para as informações apresentadas e discutidas ao longo desta monografia. Será mostrada em tal seção a teoria da interdependência complexa, assim como a definição de ciberespaço e dos elementos que a ele pertencem.

A teoria da interdependência complexa ganhou notoriedade ao questionar conceitos clássicos realistas tidos como definitivos, tais quais o Estado como único ator relevante no SI ou a segurança internacional como o tópico mais importante para o debate acadêmico. O estudo dessa teoria ajuda na compreensão dos fenômenos atuais que englobam o Estado moderno e o ciberespaço.

Para uma melhor organização, a seção será dividida em dois subcapítulos: o primeiro referente a Teoria da Interdependência Complexa, e o segundo ao Ciberespaço e suas principais características.

2.1 TEORIA DA INTERDEPENDÊNCIA COMPLEXA E O CIBERESPAÇO

A Teoria de Interdependência Complexa surgiu a partir da obra Poder e Interdependência: A Política Mundial em Transição, escrita por Joseph S. Nye e Robert O. Keohane. A teoria foi criada em meados dos anos 1970 como uma alternativa necessária à teoria hegemônica, durante os anos 1950 e 1960; o realismo clássico.

Graças às mudanças trazidas por uma sociedade cada vez mais globalizada, teorias realistas e idealistas tornaram-se incapazes de explicar de maneira satisfatória as novas dinâmicas surgindo nas relações internacionais. Problemas como o da degradação ambiental, correntes migratórias, refúgios, terrorismo, proliferação de armas, pandemias, instabilidade financeira, entre outros, trouxeram consigo uma infinidade de problemas que se provaram além do que teorias clássicas eram capazes de raciocinar.

A partir disso, Keohane e Nye, incomodados com a incompetência das teorias tradicionais, buscaram desenvolver uma teoria alternativa da política mundial, integrando liberalismo e realismo e tornando-a mais precisa e adequada àquela que chamavam de nova era das RI.

De acordo com Estre (2011), entretanto, é preciso primeiro esclarecer que o que Keohane e Nye se referem como realismo diverge dos conceitos de autores como Carr, Morgenthau ou Krasner, e, na verdade, corresponde a três pressupostos específicos. Estes são: que os Estados são unidades coesas e as mais relevantes da política internacional; que a agenda política internacional é organizada em uma hierarquia rígida, dirigida por questões de segurança (*high politics*); o uso da força é sempre um instrumento de política disponível e efetivo (ESTRE, 2011).

Com isso, os autores constroem sua antítese ao realismo

> Como seria o mundo se três pressupostos básicos do realismo fossem invertidos. Esses pressupostos são que os estados são os únicos protagonistas importantes, a força militar é o instrumento dominante e a segurança é a meta dominante. Ao contrário, podemos postular uma política mundial muito diferente: 1) os estados não são os únicos protagonistas importantes – protagonistas transnacionais atuando através das fronteiras de estados são os maiores agentes; 2) a força não é o único instrumento importante – a manipulação econômica e o uso de instituições internacionais são os instrumentos dominantes; e 3) a segurança não é a meta dominante – a guerra é a meta dominante. Podemos rotular esse mundo antirrealista de interdependência complexa. (KEOHANE; NYE JR., 1988, p. 264).

Segundo Cademartor (2016), a interdependência complexa desafia a hierarquia de questões políticas e levanta a ideia de que o poder internacional tem várias dimensões e não exclusivamente a segurança dos Estados, se tornando uma alternativa para a escola realista que havia prevalecido durante as décadas da Guerra Fria. O autor afirma que a teoria procura compreender as condições sob as quais são formadas redes de interdependência que favorecem o surgimento de instituições internacionais que por sua vez reduzem os riscos de guerras (CADEMARTOR, 2016).

Nye Jr. referia-se à interdependência como “situações nas quais os protagonistas ou os acontecimentos em diferentes partes de um sistema afetam-se mutuamente” (NYE JR., 2009, p. 250-251). Para que se constitua uma relação de interdependência, então, é necessário que haja uma dependência mútua entre dois atores, onde essa relação implique benefícios, e também, possivelmente, custos e constrangimentos recíprocos. Nesse sentido, os benefícios representam o ganho de um Estado em cima da perda de outro, enquanto custos representam a sensibilidade a curto prazo ou uma vulnerabilidade a longo prazo de cada estado (KEOHANE; NYE JR., 1988).

> A sensibilidade refere-se à quantidade e ao ritmo dos efeitos da dependência, isto é, com que rapidez as mudanças numa parte do sistema produzem mudanças em outra parte, ou seja, o grau de resposta a uma mudança no contexto político. Já a vulnerabilidade diz respeito aos custos relativos de

> mudar a estrutura de um sistema de interdependência, isto é, a mudança na política ou nas regras do jogo. (CADEMARTOR, 2016, p. 2).

A interdependência é também caracterizada pela assimetria de dependência entre Estados. De acordo com Nye Jr., tal efeito se torna uma fonte de poder quando uma entre duas partes interdependentes é menos pendente que a outra, desde que ambas valorizem a relação de interdependência (NYE JR., 2009, p. 256).

Com base nisso, é importante ressaltar a forma como Keohane e Nye Jr. enxergavam o poder internacional. Em sua concepção, o poder era rejeitado em sua definição tradicional, apenas como reflexo das capacidades militares de um Estado, e os autores abraçavam a ideia do processo de barganha. Este último corresponde ao potencial de influência que determinado ator possui sobre o resultado de negociações. Os recursos de poder, então, vão além dos recursos militares, englobando elementos como o apoio da opinião pública nacional ou internacional, a importância de seus aliados políticos, meios econômicos e seu peso em organizações internacionais (ESTRE, 2011).

A interdependência complexa apresenta três características fundamentais que a colocam em direta oposição às teorias realistas; múltiplos canais de contato, ausência de hierarquia entre as questões e o reconhecimento da força não militar (CADEMARTOR, 2016).

A primeira diz respeito ao fato de que Keohane e Nye Jr. reconhecem múltiplos canais conectando as sociedades além das relações interestatais

> Tais canais incluem relações informais entre elites políticas, arranjos formais de representantes de relações exteriores, ligações entre elites não governamentais e organizações transnacionais. São arranjados em três vertentes: (1) interestatais, tal como são tradicionalmente concebidos pelos realistas; (2) transgovernamentais, que surgem ao quebrar-se a ideia de que o Estado é uma unidade coesa; (3) transnacionais, que se referem aos outros atores da política mundial além dos Estados (ESTRE, 2011, p. 39).

Incontáveis consequências emergem a partir destes novos meios de contato ao passo em que eles aumentam a sensibilidade e a vulnerabilidade dos Estados. Cada vez mais, políticas econômicas estrangeiras afetam ou são afetadas por políticas domésticas, borrando a linha entre política externa e interna conforme o escopo das atividades dos governos se amplia, e conforme corporações e bancos tomam decisões que transcendem as decisões nacionais (KEOHANE & NYE, 1989).

A segunda característica essencial à interdependência complexa é o reconhecimento de que não existe uma hierarquia definida a partir de tópicos dentro das discussões internacionais. A existência de questões rivais como energia,

recursos, meio-ambiente, população, uso de espaços e mares fazem com que a segurança não domine os demais itens. Além disso, os departamentos de agricultura, comércio, defesa, saúde, educação, entre outros têm ramificações internacionais que se sobrepõem umas às outras (CADEMARTOR, 2016).

Por fim, contrário ao realismo, o poder militar não seria um instrumento de política efetivo contra outros Estados dentro da interdependência complexa. Contudo, ele ainda é relevante nas relações com os demais Estados que estejam fora da região ou em outros temas. O principal motivo para isso é que o uso da força frequentemente impõe custos aos outros objetivos estatais além da segurança. Utilizar a força militar contra determinada nação pode fazer com que relações em outras áreas temáticas sejam rompidas, causando prejuízos que podem ser significativos. Uma alternativa a esse problema, como apontado pelos autores, seria o uso de instrumentos econômicos como força de persuasão (ESTRE, 2011).

Estas três características, em conjunto, fazem com que surjam novos processos políticos distintos daqueles esperados dentro do ideário realista. Dentre estes, quatro novos processos podem ser destacados:

Em primeiro lugar, os Estados mais fortes não poderiam sempre utilizar de meios militares para atingirem seus objetivos e seria possível que um Estado agregasse diversos temas da agenda internacional para que fossem negociados conjuntamente em busca de influência sobre os resultados das transações. Atores mais fracos poderiam também utilizar desta estratégia de agregação para conseguir maior capacidade de ação, como foi o caso da Organização dos Países Exportadores de Petróleo (OPEP) (ESTRE, 2011).

Em seguida, o fato de não haver uma hierarquia definida de temas, em conjunto com o crescimento de regimes e organizações internacionais, tornaria imprescindível a formação e o controle da agenda das negociações globais.

Em terceiro lugar, as relações transnacionais e transgovernamentais tornam difícil a distinção entre política interna e internacional. E por último, as organizações internacionais teriam um papel fundamental na política mundial (ESTRE, 2011).

Em conclusão a esse subcapítulo, nesta monografia pretende-se utilizar da Teoria de Interdependência Complexa de Keohane e Nye Jr. como pilar fundamental para demonstrar a maneira como o mundo cibernético vem influenciando cada vez mais a tomada de decisão dos Estados. Os múltiplos canais de contato que emergem entre as sociedades não só proporcionam instrumentos de influência para os

governos, mas também para que os atores não governamentais exerçam influência sobre as regências. O ciberespaço entra como uma das principais fontes de novos canais de contato.

2.2 CIBERESPAÇO E SEUS PRINCIPAIS ELEMENTOS

A internet e, portanto, o ciberespaço, surgiu em meio ao auge da Guerra Fria, durante a década de 1960, como uma forma de garantir segurança para os dados sensíveis americanos. Pesquisadores do Massachusetts Institute of Technology (MIT), da Universidade de Stanford e da Universidade da Califórnia, financiados pela Agência de Projetos e Pesquisas Avançadas do Departamento de Defesa dos Estados Unidos (DARPA), criaram a ARPANET, uma rede para comunicação entre computadores dessas universidades e, também, para o DARPA (MESQUITA, 2019).

> [...] a necessidade de proteger o território estadunidense fez com que um grupo de pesquisadores criassem a Intergalatic Computer Network, o embrião da internet (SANTOS, 2011). Isso possibilitou a conexão com as ideias de Hindemburgo Francisco Pires (2012, p.3), para o qual a posterior criação da ARPANET possibilitou a interconexão entre “as empresas privadas, as universidades, centros de pesquisas e laboratórios.” (SANTOS, 2011 apud RIGAMONTE, 2017, p. 8).

Com o passar do tempo, graças ao apoio financeiro do setor empresarial e a ajuda de universidades, o ciberespaço evoluiu a partir de novas redes, códigos e protocolos que permitiram a criação da internet como conhecemos hoje. Conforme o ciberespaço se expandiu, tornou-se claro para os Estados o valor comercial e político do controle das informações que circulam nessa rede (RIGAMONTE, 2017).

Entre o período de 1996 até 2017, a quantidade de usuários da internet foi de 36 milhões para 3,7 bilhões. Segundo Nye, o ciberespaço faz-se cada vez mais presente no cenário político, econômico e social, gerando uma interdependência que, por sua vez, trouxe desenvolvimento e oportunidades econômicas, mas, também, vulnerabilidade e insegurança (NYE, 2018).

O desenvolvimento mais extraordinário da nova era digital foi o de um conjunto interconectado e padronizado de redes globalizadas de computadores e dispositivos de comunicação. Estas redes se tornaram uma arena global de interação para infinitas atividades compartilhadas e para a troca de informações e ideias por pessoas ao redor do mundo, envolvendo uma fração considerável da humanidade no dia a dia (REARDON, CHOUCRI, 2012).

Apesar de terem sido usados até o presente momento de forma análoga, é preciso definir que os conceitos de internet e ciberespaço se diferem, pois apesar de incluir a *World Wide Web* (WWW) em seu escopo, o ciberespaço engloba, muito além disso, tudo aquilo conectado a qualquer rede de computadores no mundo. Longe de ser um ambiente puramente virtual, o mundo cibernético é composto por uma série de elementos físicos como as máquinas que armazenam os dados, a infraestrutura que possibilita o fluxo desses dados e, até, pessoas que estão por trás dos computadores e demais dispositivos conectados ao ciberespaço (MESQUITA, 2019).

Como um domínio moldado pela experiência do usuário e pelos avanços tecnológicos, o ciberespaço está em constante mudança. Portanto, sua definição não é definitiva e precisa ser atualizada regularmente, já que um número crescente de atores forma e transforma o conceito. Como Rattray (2009, p.256) afirmou "montanhas e oceanos são difíceis de mover, mas partes do ciberespaço podem ser ativadas e desligadas com o toque de um interruptor; eles podem ser criados ou 'movidos' por inserções de novas instruções codificadas em um roteador ou *switch*". Assim como Nye (2012, p. 164) escreveu, “o domínio cibernético é único, pois é feito pelo homem, é recente e está sujeito a mudanças tecnológicas ainda mais rápidas do que outros domínios” (RATTRAY, 2009, NYE, 2012 *apud* MESQUITA, 2019).

Dentro da Doutrina Militar de Defesa Cibernética (BRASIL, 2014, p. 18), o Exército Brasileiro define o espaço cibernético como um "espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas". O documento, publicado pelo Ministério Federal do Interior da Alemanha e intitulado *Cyber Security Strategy for Germany* , define o ciberespaço como “[...] uma rede de conexão e transporte universal e acessível ao público, que pode ser complementada e ampliada por qualquer número de redes de dados adicionais [...]” (ALEMANHA, 2021, p. 9). Por outro lado, o Dicionário de Termos Militares e Associados do Escritório do Presidente do Estado-Maior Conjunto (DOD, 2019, p. 55) dos EUA, define o ciberespaço como um domínio global dentro do ambiente de informação, que consiste em uma rede interdependente de infraestruturas de tecnologia da informação (TI) e dados residentes, incluindo a Internet, redes de telecomunicações, sistemas de computadores e processadores e controladores incorporados (MESQUITA, 2019).

A documentação de defesa de diversos países enxerga o domínio cibernético como um espaço dependente da interconectividade de elementos físicos que

permitem a criação de uma rede global de informação. Esta cadeia gera uma dependência pelo ciberespaço que os Estados agora caracterizam como essencial para segurança e defesa (MEDEIROS, 2020).

> Dessa forma, o ciberespaço pode ser entendido como um domínio único de interação humana artificial, dissociado em parte dos elementos físicos, que permeiam os domínios tradicionais. Ele existe através da conexão de diferentes camadas: tecnológica, técnica e pessoal. Tem peculiaridades únicas, tornadas possíveis por sua imaterialidade parcial e interconexão expansiva. O ciberespaço está em constante evolução à medida que a tecnologia avança, e está em constante mudança à medida que diferentes atores o utilizam, moldando-o para atender às mais diversas necessidades (MEDEIROS, 2020, p. 23).

O ciberespaço é considerado um domínio único porque, ao contrário dos espaços naturais, ele foi criado pelo homem. Além de existir no espectro eletromagnético, o ciberespaço é ancorado pela eletrônica que funciona como nós envolvidos em uma rede expansiva destas máquinas, que são conectadas por dados binários enviados de um para outro. Ao conectar equipamentos, tecnologias e atores através do ciberespaço, novos significados são dados à rede, que se transforma posteriormente em um sistema de armas estratégicas, um meio para demonstrações sociais através de redes sociais e um ambiente comercial para instituições financeiras, empresas e clientes, entre outros (MEDEIROS, 2020).

2.2.1 A trindade do ciberespaço

Em sua dissertação, Medeiros (2019) desenvolveu uma ferramenta analítica composta por três elementos conceituais inerentes ao ciberespaço com o objetivo de testar a adaptabilidade de preceitos das diferentes correntes teóricas de RI na medida que a sociedade se torna mais dependente do mundo cibernético. O autor intitulou esta ferramenta de Trindade Conceitual Fundamental do Ciberespaço, cujos elementos são a desterritorialidade, a multiplicidade de atores e a incerteza. A combinação destes desestabiliza as concepções fundamentais de território, Estado como detentor exclusivo da força e *accountability* (MEDEIROS, 2019).

A seguir serão apresentados cada um dos elementos delineados.

2.2.1.1 Desterritorialidade

A característica mais notável do ciberespaço é o rompimento das concepções clássicas de território, como o espaço físico delimitado por fronteiras. O território nacional é comumente definido como a área onde o Estado atua garantindo sua legitimidade e o poder sobre seus recursos, servindo como base geográfica de sua soberania. Complementar a esta ideia é o conceito de territorialização, onde diferentes grupos exercem poder sobre uma área precisa, delimitando-a e tendo os limites reconhecidos por outros grupos (MEDEIROS, 2019).

> O processo de territorialização corresponde à "tentativa de um indivíduo ou grupo de alcançar, influenciar ou controlar pessoas, fenômenos e relacionamentos, delimitando e afirmando o controle sobre uma área geográfica" (Haesbaert 2002: 119). O instrumento para delimitar e controlar o acesso a uma área geográfica é a fronteira, que permite a entrada de alguns e exclui outros. Neste sentido, o território assume o caráter de uma zona. Ou seja, a delimitação de fronteiras pelo processo de territorialização dá origem a uma certa zona na qual o poder é exercido, transformando-o em um território (HAESBAERT, 2002 *apud* MEDEIROS, 2020, p.25).

Redes comerciais, criminosas e financeiras fazem parte de um novo fenômeno trazido pela globalização atual, conhecido como as novas redes globais, que por sua vez penetram e interconectam diferentes territórios. Essas redes podem ser definidas como matrizes de infraestruturas técnicas densas e interconectadas que possibilitam novas formas de organização territorial da sociedade (COELHO NETO, 2013 apud MEDEIROS, 2020).

O domínio cibernético compõe sua própria rede global constituída por uma camada física — na forma de cabos, satélites e dispositivos interconectados — e por uma camada imaterial, na forma de um fluxo constante de informações digitalizadas. Dessa forma, enquanto dispositivos físicos estão inseridos em territórios, os fluxos que interconectam esses aparelhos transpõem os limites fronteiriços de diferentes zonas territoriais. A imaterialidade do ciberespaço lhe garante livre circulação no mundo globalizado, atravessando fronteiras livremente e penetrando territórios sem grande dificuldade (MEDEIROS, 2019).

O território físico perde, então, sua ligação exclusiva a uma territorialidade material. Esta última agora se manifesta nos fluxos das relações sociais dentro do mundo cibernético, legitimando-o como espaço de poder no século XXI. A lógica reticular do ciberespaço enfraquece a lógica zonal do território e, por se tratar de um espaço de poder sem delimitações físicas que não obedece aos pressupostos fundamentais do território, passa ser dotado de um caráter desterritorializado. “Dessa

forma, atos realizados em dispositivos fisicamente localizados em um determinado território podem ter efeitos ou consequências em outros territórios, sob a soberania de outros Estados, mas que estão conectados à mesma rede" (MEDEIROS, 2019, p. 28).

2.2.1.2 Multiplicidade de Atores

Conforme o domínio cibernético se torna um legítimo espaço de poder, o número de atores capazes de acessar e interagir com esse novo domínio de poder cresce exponencialmente. Atualmente, mais da metade da população mundial, não apenas possui acesso ao ciberespaço, mas é direta ou indiretamente influenciada pelo mundo cibernético (MEDEIROS, 2019).

Os setores militares e governamentais passaram a utilizar do ciberespaço também como um domínio de projeção de poder análogo aos domínios terrestres, marítimos, aéreos e espaciais, operacionalizando-o para situações de ataque e defesa. Eles utilizam de redes de comunicação para tornar mais autônoma e interconectada a infraestrutura do país, assim como para gerir os sistemas de armas e contingentes das forças armadas. Entretanto, à medida que mais componentes críticos para o funcionamento de diferentes setores da sociedade passam a depender do ciberespaço e o número de atores nesse domínio cresce, os setores militares e governamentais deixam de ser a única ameaça com capacidade de explorar esse domínio (MEDEIROS, 2019).

Tal fenômeno interliga diferentes atores capazes de utilizá-lo de maneiras diferentes. Indivíduos ou grupos dotados do conhecimento e de dispositivos interconectados estão aptos a explorar a dependência do ciberespaço de acordo com suas próprias agendas, seja na forma de crimes cibernéticos, ciberterrorismo, sabotagem, espionagem, monitoramento, entre outros (MEDEIROS, 2019).

> Ao contrário dos domínios tradicionais, o ciberespaço permite a redução do distanciamento de capacidades entre diferentes atores. Nye (2012) se refere a esse fenômeno como a "difusão de poder" a qual é "representada pelo vasto número de atores envolvidos e pela relativa redução dos diferenciais de poder entre eles" (NYE, 2012, p.173). Ou seja, novos atores possuem a capacidade de exercer a força no domínio cibernético, por meio de ações com o intuito de prejudicar infraestrutura, pessoas e/ou instituições. Apesar da permanência de uma perspectiva legal do Estado como detentor exclusivo da força, a difusão de poder permite o exercício prático da força por grupos de hackers, ativistas, criminosos, terroristas, ou qualquer indivíduo ou grupo com dispositivos conectados que podem vir a explorar a crescente dependência mundial do ciberespaço (NYE, 2012 *apud* Medeiros, 2019, p.31).

A difusão de poder pode se manifestar no ciberespaço de duas maneiras; como meio de exploração em si, pois o conhecimento técnico permite que atores utilizem *softwares* capazes de atacar determinados alvos por intermédio de linhas de código, criando assim armas cibernéticas que podem ser vendidas e difundidas pela rede para quem estiver interessado. A segunda maneira se refere aos meios de comunicação; o alcance global do ciberespaço permite que dissidentes, criminosos, indivíduos, grupos e instituições com diferentes ideologias, interesses e objetivos possam se fazer ouvidos ao redor do mundo. Organizações terroristas podem expandir suas operações através de indivíduos de países distantes, criminosos podem controlar o tráfico de drogas e armas mesmo encarcerados, e jornalistas podem contatar fontes anônimas a milhares de quilômetros de distância (MEDEIROS, 2019).

Mesmo que governos ainda detenham o maior controle sobre o mundo cibernético, a difusão de poder permite que Estados fragilizados, dissidentes, separatistas, terroristas, ativistas e militares, como uma forma de compensar fraquezas em armamentos e capacidades de poder tradicionais, possam utilizar do mesmo para perpetrar missões e ataques. “É mais inteligível e barato um grupo de hackers perpetrar um ato de sabotagem cibernética contra uma usina elétrica do que treinar homens, adquirir e operar um grupo de blindados, para que a usina seja desestabilizada por meios cinéticos convencionais, por exemplo”. (MEDEIROS, 2019, p. 32)

Graças ao baixíssimo custo de entrada e operação no domínio cibernético se comparado a outros, este se torna um *locus* de relações de poder por múltiplos atores que passam a perseguir seus interesses no novo domínio. Enfim, a sociedade internacional deixa de ser o palco monopolizado por atores governamentais e novos jogadores se inserem no tabuleiro das relações internacionais (MEDEIROS, 2019).

2.2.1.3 Incerteza

A incerteza do domínio cibernético é um dos elementos que mais constrange os setores governamentais e militares. Ela reflete a dificuldade de atribuição de ações realizadas no ciberespaço devido à complexidade da rede e ao fator anonimato.

Em razão da complexidade de tal espaço, torna-se extremamente difícil atribuir uma relação de causa e efeito a determinado evento no ciberespaço. Raramente é possível traçar uma linha até uma ação causadora específica, principalmente porque os efeitos de determinada ação não são necessariamente cinéticos ou imediatos. Por

outro lado, o anonimato reflete justamente a impossibilidade de atribuição de ações a atores específicos em determinados lugares. Sem a capacidade de atribuição, é impossível iniciar o processo legal e político de responsabilização e eventual *accountability* (MEDEIROS, 2019).

Como consequência da dificuldade de atribuição de fluxos anônimos no ciberespaço, a incerteza se manifesta podendo ocasionar sérios conflitos nas relações internacionais, como um contra-ataque a possíveis oponentes não necessariamente culpados, levando à escalada descontrolada do conflito. O pressuposto da ambiguidade em tal fenômeno gera desafios teóricos e práticos não apenas para as relações internacionais, na forma de conflitos, manifestações, crises e outros desenvolvimentos do cenário global, mas, também, para áreas mais específicas dessas ligações como economia e direito internacional, tendo como exemplo, a utilização de moedas criptografadas não rastreáveis, como a *bitcoin*, para diferentes atividades ilícitas (MEDEIROS, 2019).

2.2.2 *Big Data*

Big Data é um termo usado desde a década de 1990 e que representa pacotes de dados em tamanhos que não podem ser manuseados por computadores comuns em uma duração de tempo prática. A dimensão de arquivo que encaixe a definição tem aumentado constantemente ao longo dos anos conforme o poder de processamento dos computadores modernos tem crescido, de alguns terabytes em 2012 até vários zettabytes atualmente. (ZWITTER 2015).

O *Big Data* como objeto de estudo é um fenômeno recente e que ainda está se desenvolvendo dentro do mundo acadêmico. Mesmo assim, existem autores que se propuseram a estudar essa nova tecnologia e suas implicações. Zwitter (2015) definiu, em seu trabalho, o fenômeno como enormes quantidades de dados que, usando analíticas sofisticadas, podem ser mineradas para obter informações, a fim de revelar padrões e detectar tendências e correlações. Diferente de amostras limitadas em pesquisas tradicionais, o *Big Data* possui a capacidade de extrair e interpretar informações de quantidades maciças de dados não estruturados (ZWITTER 2015).

De acordo com Silva (2018), dados coletados através do *Big Data* se diferem de pesquisas de amostragem tradicionais pois, além de serem ilimitados em espaço, tempo, tamanho, e estarem organizados em inúmeras fontes constantemente

monitoradas, expressam a realidade nua e crua, traduzem atitudes, ações humanas, e não convicções. O que, na sociedade digital, pode valer mais que petróleo (SILVA, 2018).

A maioria dos autores definem três importantes características para se compreender *Big Data*, sendo elas volume, velocidade e variedade.

O primeiro diz respeito ao fato de se produzirem mais dados diariamente do que o cérebro é capaz de compreender. Enquanto desde o início da história até 2011 foram produzidos cinco bilhões de *gigabytes* de informação, em 2015 este volume era produzido diariamente. Pacotes de dados estão sendo medidos agora em *yottabytes*, o equivalente a 250 trilhões discos de vídeo digital (ZWITTER 2015).

Velocidade se refere a criação e coleção de dados que agora acontece em tempo real. Através de uma banda larga maior e da implementação de arquiteturas digitais capazes de fazer sentido dessa velocidade e volume (ZWITTER 2015).

A última característica, variedade quer dizer a quantidade de fontes e formatos diferentes de dados que podem ser coletados, assim como a diversidade de formas que esses dados podem ser categorizados. Tais podem ser estruturados ou não; advir de fontes como e-mails, fotos, documentos, vídeos, áudios; e podem ser classificados como autogerados da internet ou como extraídos de fontes externas (ZWITTER 2015).

A partir de suas peculiaridades, o *Big Data* se torna uma ferramenta que fornece vantagens em termos de informação, seja de negócios, estatal, ou de qualquer outra natureza. Aquele que souber utilizar desse novo fenômeno possui a capacidade de, ao menos em teoria, tornar se onisciente, o que qualquer organização, seja ela lícita ou ilícita, deseja.

> O processo de mineração de dados, ou *data mining*, fornece *insights* sobre comportamentos e motivações humanas, tendências sociais, mudanças ambientais, dentre outras informações necessárias à predição, previsão e antecipação, gerando entusiasmos tanto sobre os setores empresariais que se utilizam dessas informações para prever e antecipar gostos, preferências e desejos dos consumidores, quanto aos setores político estratégico-militares do Estado que se valem dessas informações para construir inteligência e dar continuidade à operações militares e estratégicas (ASSIS, 2020, p. 18).

De acordo com Chandler (2015), *Big Data e,* por conseguinte, a Internet das Coisas que veremos na subseção seguinte, transforma a maneira como interagimos com o mundo ao nosso redor. A dataficação de nossas rotinas, conforme a autora coloca, é o cerne desse novo fenômeno. Tal conceito é uma ferramenta que nos permite observar a realidade sob uma nova perspectiva ao tornar simples interações

e relações em dados quantificáveis e capazes de serem analisados. Podendo-se extrair fortes correlações desses dados (CHANDLER, 2015).

Diferente de pesquisas tradicionais, o *Big Data* primeiro coleta informações a partir de pacotes massivos de dados, extraídos de nossas pegadas digitais, e somente após a coleta que uma hipótese é construída. Ao invés de buscar dados para testar uma teoria, pesquisadores agora podem criar uma teoria a partir das informações (CHANDLER, 2015).

2.2.3 Internet das Coisas

Cunhado pela primeira vez em 1999 por Kevin Ashton, a Internet das Coisas é um conceito que segundo Faccioni Filho (2016) não faz parte do âmbito das tecnologias. Na realidade, engloba uma série de inteligências modernas e as utiliza para cumprir uma série de funcionalidades (FACCIONI FILHO, 2016).

A teoria surgiu do desenvolvimento de várias áreas como sistemas embarcados, microeletrônica, comunicação e sensoriamento; como uma extensão da Internet, permitindo que objetos do dia a dia possam se conectar ao ciberespaço. Esse novo fenômeno permite que objetos se comuniquem com pessoas e com outros objetos, criando uma série de oportunidades de inovação (SANTOS; SILVA; CELES; BORGES NETO; PERES; VIEIRA; VIEIRA; GOUSSEVSKAIA; LOUREIRO, 2016).

O número de dispositivos e equipamentos conectados à internet, como computadores, celulares, automóveis, televisores e eletrodomésticos, cresce cada vez mais. A Internet das Coisas possibilita detectar o contexto desses dispositivos, controlá-los, viabilizar a troca de informações uns com os outros, acessar serviços da Internet e fazê-los interagir com pessoas. A partir disso, surge, por exemplo, a ideia de se construir cidades e casas inteligentes, capazes de se comunicarem com seus habitantes e capazes de serem controladas de forma remota (SANTOS; SILVA; CELES; BORGES NETO; PERES; VIEIRA; VIEIRA; GOUSSEVSKAIA; LOUREIRO, 2016).

> Assim, a Internet das Coisas torna-se cada vez mais pervasiva, inteligente e interativa. Atualmente, além das usuais interfaces utilizadas pelos humanos em seu dia a dia, como smartphones, tablets, desktops, milhares de outras aplicações têm sido desenvolvidas: por exemplo, pombos com RFID[1]

[1] A identificação por radiofrequência é a utilização de campos eletromagnéticos para identificar e rastrear automaticamente etiquetas fixadas em objetos. Um sistema RFID consiste em um pequeno transponder de rádio, um receptor e um transmissor de rádio.

> implantados e sensores enviam informações sobre a poluição do ar via internet; médicos podem monitorar o estado de saúde dos pacientes à distância; a indústria farmacêutica pode combater largamente a falsificação; governos visualizam o movimento das pessoas nos pedágios e alfândegas; lojas controlam remotamente e em tempo real entradas e saídas de mercadorias assim como sua localização em trânsito; sensores percebem a umidade da terra e informam quando as plantas precisam ser regadas (GALA, 2013, p. 29).

A ideia de ubiquidade representa muito bem o conceito, se referindo a algo presente em todos os momentos e em todos os lugares, persistente, sempre disponível e atuante. Assim como o ciberespaço, ela supera noções tradicionais de espaço físico, ocorrendo de forma simultânea em lugares diferentes (GALA, 2013).

2.3 O SISTEMA INTERNACIONAL

Por último, um conceito essencial para a compreensão da seguinte dissertação é o de SI. E, assim, como todo e qualquer conceito dentro do debate acadêmico de RI não é possível encontrar uma definição concreta e inviolável de SI, cada corrente teórica dentro do campo das RI o enxerga de maneira diferente. Entretanto, ainda é possível notarmos certas características compartilhadas entre as diferentes visões.

Em termos brandos, o SI pode ser definido como o espaço abstrato que contempla todos os atores e eventos que compõem as relações internacionais. Esse sistema é anárquico, mas não caótico, e nele o comportamento dos atores, tanto estatais como não-estatais, é limitado por uma ordem internacional que, embora não possua normas e regras por escrito, está carregada de conteúdo normativo (MONTENEGRO, 2013).

Para os autores realistas, o SI é um sistema anárquico onde não há uma hierarquia geral entre Estados soberanos e no qual esses são os únicos atores relevantes para a existência do sistema. Por mais que haja uma divergência entre os realistas se o Estado é capaz de moldar ou se ele é moldado pelo SI, todos concordam que polaridade e equilíbrio de poder são elementos fundamentais de seu funcionamento, e que somente através de mudanças no equilíbrio de poder vigente que o sistema seria capaz de ser alterado. Dentro da concepção realista, os eventos ou descobertas que poderiam gerar uma revolução dentro do sistema seria uma grande guerra, tal qual a Segunda Guerra Mundial, ou uma nova tecnologia como a invenção da bomba nuclear (MINGST, 2014).

Entretanto, esta dissertação será baseada primordialmente na visão liberal sobre o SI, que o entende não como uma estrutura imutável, mas como um sistema interdependente no qual ocorrem múltiplas e fluidas interações entre diferentes partes, e no qual vários atores aprendem com a interação. Para os autores de tal teoria, o Estado não configura o único ator significativo no SI, dando lugar para organizações governamentais internacionais, organizações não-governamentais e corporações multinacionais. Uma das características essenciais que concerne o SI, de acordo com a visão liberal, é o multilateralismo e a forma que ele coordena a ação dos atores dentro sistema partindo dos princípios de segurança coletiva onde a guerra contra um é contra todos (MINGST, 2014).

Por fim, os autores liberais definem que a mudança dentro do sistema pode ocorrer por uma multiplicidade de razões. Uma delas seria pelo desenvolvimento tecnológico exógeno, independente de atores do sistema, como desenvolvimentos em tecnologias de informação e comunicação. Outra, por mudanças em campos como economia, direitos humanos ou meio-ambiente. E, uma última, seria pela introdução de novos atores de diferentes naturezas dentro do sistema, no qual poderiam desenvolver novos tipos de relações e afetar o comportamento tanto do SI quanto dos Estados (MINGST, 2014).

3 A EMERGÊNCIA DE ATORES NÃO-ESTATAIS NO CIBERESPAÇO E SUA INFLUÊNCIA SOBRE O SISTEMA INTERNACIONAL

Ao longo deste capítulo será analisado com maior detalhe as formas como atores não-estatais ameaçam a soberania do Estado através do ciberespaço. Serão debatidos fenômenos tais quais o ciberterrorismo, o cibercrime, a ciberguerra e o hacktivismo. Também serão descritos múltiplos ataques cibernéticos significativos na história.

Em um segundo momento, ocorrerá uma reflexão sobre a utilização do ciberespaço por grandes corporações do ramo de tecnologia da informação e a forma como essas utilizam do mundo digital para desafiar a soberania descrita anteriormente. Será explorado o caso da *Cambridge Analytica* (CA) e sua influência sobre as eleições presidenciais dos EUA de 2016.

Por último, será realizada uma recapitulação dos principais pontos debatidos, trazendo uma reflexão sobre o impacto dessas considerações no SI.

3.1 O CIBERESPAÇO COMO UMA AMEAÇA À PAZ

Como foi possível de observar ao longo do marco teórico conceitual desta obra, o mundo cibernético se tornou definitivamente um espaço que contempla infinitas possibilidades de criação e de ação sobre praticamente todos os aspectos de nossas vidas. Graças às revoluções em informação e tecnologia, hoje possuímos uma qualidade de vida inédita na história da humanidade e possuímos acesso a incontáveis inovações que antigas gerações podem apenas sonhar em ter.

Desde avanços em saúde como cirurgias robóticas assistidas ou a impressão de órgãos 3D, até avanços em áreas ordinárias como casas inteligentes e carros autônomos, vivemos cercados por constantes avanços e novos desenvolvimentos em ciência e tecnologia que acontecem em um ritmo sem precedentes. Hoje, a velocidade de propagação de informação é tão rápida que grandes descobertas na ciência tornaram-se rotineiras.

Estes saltos em tecnologia continuam a facilitar nossas vidas e a solucionar problemas que sempre consideramos impossíveis — graças ao desenvolvimento do domínio cibernético. Este último trouxe significativas mudanças para a sociedade que transformaram a maneira como nos relacionamos uns com os outros. Dentre essas modificações, devemos citar a forma como o ciberespaço é capaz de empoderar indivíduos e grupos minoritários e ajudar causas humanitárias e sociais. Como afirmou Zwitter (2015), à medida que o *hardware* se torna melhor e mais barato, e à medida que *softwares* de código aberto e serviços de busca e análise de banco de dados se tornam mais acessíveis, indivíduos e grupos pequenos ganham a oportunidade de agir através do mundo cibernético.

As tecnologias de informação e comunicação têm sido vistas há muito tempo como fomentando a formação de uma "sociedade civil global", ou seja, um conjunto de grupos civis e transnacionais que existem e funcionam fora do controle dos Estados. Juntas essas redes, alavancando o poder do ciberespaço, poderiam conseguir uma remodelação significativa da política mundial, promovendo a paz internacional e as normas democráticas (REARDON, CHOUCRI, 2012).

Um grande exemplo possível de se observar é o caso de como a tecnologia cibernética capacitou as mulheres no mundo árabe, fornecendo-lhes um fórum acessível para expressão política. A abertura e o anonimato do ciberespaço deram a essas mulheres uma voz que de outra forma não teriam, e tal fato está começando a ter um efeito positivo sobre a posição das mulheres na sociedade árabe. Da mesma maneira, o ciberespaço está ajudando a criar uma área online para o diálogo livre e para a expressão de ideias no mundo árabe, o que pode servir como uma poderosa crítica à autoridade estatal, algo que nunca existiu anteriormente na região (REARDON, CHOUCRI, 2012).

Como Nye Jr. (2002) defendeu, o acesso de novos atores a rápidos avanços tecnológicos em computadores, comunicações e *softwares* ocasiona um processo de difusão de poder, caracterizado pela passagem de muitas atividades para fora do controle estatal. Esse processo altera a relação entre população e governo como uma forma de estreitar laços e modernizar a relação do Estado com a população, ampliar o papel das organizações sem fins lucrativos e aprofundar um fortalecimento democrático (MAIER, 2016).

> [...] isso implica que as populações dos países possuem agora maiores e melhores meios de comunicação, rompendo o controle estatal e das grandes empresas transnacionais. Esse acesso à informação gera por sua vez uma

> maior capacidade de mobilização que tende a influenciar e pressionar mais as decisões dos governos. A associação entre a revolução da informação e a democratização é colocada por Nye e tal associação garante às sociedades civis um maior poder de influência, sobretudo nas democracias (MAIER, 2016, p. 12).

A partir disso, as capacidades de atração e persuasão advindas de minorias e indivíduos representam formas mais eficazes de agir num ambiente mais complexo, no qual os governos devem prestar contas diante de suas populações cada vez mais empoderadas pela revolução da informação (MAIER, 2016). Qualquer cibernauta pode atuar em nome de um ideal e alterar o destino das relações internacionais a partir da internet — assim como esta pode ser utilizada como um instrumento na defesa da liberdade (MESSIAS, BRANDÃO, 2013).

O mundo cibernético também se tornou um excelente instrumento usado em missões humanitárias ao redor do mundo. A fim de auxiliar as agências humanitárias e de desenvolvimento no planejamento operacional, logística e monitoramento de seus projetos, foram desenvolvidas várias plataformas que fornecem acesso aberto a dados confiáveis. Além de dar às ONGs um meio de coletar informações cruciais por conta própria, este compartilhamento de dados também pode ajudar a facilitar a prestação de ajuda (ZWITTER, 2015).

A Ushahidi, por exemplo, é uma empresa de *software* sem fins lucrativos que desenvolve sistemas operacionais livre e *open-source* para a coleta de informações, visualização e mapeamento interativo. A companhia criou um site após a disputada eleição presidencial do Quênia, em 2007, que recolheu relatos de testemunhas oculares de violência comunicados por e-mail e mensagem de texto e colocou a informação em um mapa do Google Maps. Este site foi usado, também, em apoio a operações humanitárias após o terremoto de 2010 no Haiti e na melhoria das eleições no Quênia em 2013 (o projeto Uchaguzi) (ZWITTER, 2015).

Estas novas tecnologias também estão sendo testadas por ONGs internacionais. Entre elas está o *Humanitarian Data Exchange* (HDX), um projeto lançado pelo Escritório das Nações Unidas (ONU) para a Coordenação de Assuntos Humanitários que já acumulou mais de 1.500 conjuntos de dados. Alguns exemplos incluem um conjunto para monitorar casos de Ebola e trabalhadores humanitários infectados; um para analisar as fontes de água e a qualidade da água no Quênia; e outro para registrar o total de pessoas uniformizadas de cada país membro contribuinte por mês, tipo e missão (ZWITTER, 2015).

Ao adotar sistemas de conscientização em tempo real, *feedback* e alerta precoce, pesquisadores argumentam que a utilização do *Big Data* na prevenção de conflitos e na ação humanitária levará a uma nova geração de *peacekeeping* e *peacebuilding* para a ONU. Por exemplo, as imagens de satélite estão se tornando cada vez mais uma fonte de análise através do *Big Data*. Dados geo-localizados juntamente com pesquisas, fotos e mapas podem ajudar na investigação de crimes de guerra. O Satélite Sentinel, um programa da Iniciativa Humanitária de Harvard, encontrou oito valas comuns na aldeia de Kadugli, no Sudão, em 2011 com base em imagens de satélite que foram corroboradas com relatórios da ONU e relatos de testemunhas oculares (ZWITTER, 2015).

Também é possível que o *Big Data* possa ser usado para prever conflitos e instabilidade social. Nos Estados Unidos (EUA), o programa Volume de Informação e Velocidade emprega o reconhecimento de padrões para detectar instabilidade social em populações como parte do esforço do Departamento de Defesa do país para aproveitar a inteligência estratégica do sistema (ZWITTER, 2015).

Alguns teóricos de RI enxergam, ainda, o *Big Data* como um substituto eficaz e ético para as formas tradicionais de intervenção internacional, que são vistas como muito lentas, pesadas e redutoras para se envolverem adequadamente com as realidades contextuais concretas do mundo. O *Big Data* surge, então, como uma ferramenta de comunidades locais e "sociedades civis", para gerar seu próprio conhecimento de si mesmas e para agir de acordo com ele (CHANDLER, 2015).

Ainda segundo o mesmo autor, múltiplas fontes de dados poderiam permitir que indivíduos, famílias e sociedades praticassem uma autogestão responsiva e reflexiva de maneiras que antes eram consideradas impossíveis. Assim, *Big Data* poderia potencialmente capacitar precisamente aqueles que são mais marginais e vulneráveis nos momentos de maior risco.

Entretanto, por tudo que o ciberespaço nos trouxe até agora e por tudo que ele ainda vai nos trazer, é ingênuo pensar que ele possa existir no mundo apenas de modo altruísta e inocente. Não somente o mundo cibernético é usado hoje para atender as demandas de organizações criminosas e terroristas, como muitos dos métodos em que ele pode ser usado, salientados anteriormente, variam de idealistas no melhor dos casos até perigosos no pior.

Viajando com dinheiro, pouca segurança e equipamentos caros, trabalhadores humanitários se tornam alvos fáceis para ataques de grupos ideológicos ou de grupos

criminosos em busca de lucro. Através da forma como o Ushahidi mapeia e provê informações detalhadas e estruturadas, elas podem ser utilizadas para facilmente rastrear esses agentes humanitários. Algo que grupos criminosos apenas sonhavam anos atrás. Tal foi o caso das operações após enchentes no Paquistão, em 2010, quando as forças talibãs baseadas no Paquistão ameaçaram atacar todos os trabalhadores humanitários estrangeiros, como os do Programa Mundial de Alimentos ou Médicos Sem Fronteiras (ZWITTER, 2015).

Ao mesmo tempo, é ingênuo crer que, somente através do domínio cibernético e da utilização do *Big Data*, comunidades marginais e vulneráveis poderão se auto coordenar e resolver sozinhas suas dificuldades. O *Big Data* pode ser usado para gerenciar o que já existe, por exemplo, reconfigurando redes de transporte ou energia para atender a demanda de pico ou adaptar-se a falhas de sistemas, mas não pode fornecer mais do que assistência técnica com base no que já existe. Não se pode formular estratégias eficazes e responder a ameaças associadas a questões sociais, econômicas e ambientais sem pressupostos de causalidade. As pessoas não são capacitadas pelo sistema para mudar suas circunstâncias, mas para se tornarem mais conscientes delas, a fim de se adaptarem (CHANDLER, 2015).

Outrossim, muitos autores defendem que o potencial danoso inerente ao domínio cibernético supera em muito a capacidade que o mesmo possui para a construção e o desenvolvimento de uma melhor qualidade de vida para os seres humanos. Devido à natureza intrínseca ao ciberespaço, como o baixo custo de investimento para a entrada, o anonimato virtual e a facilidade de saída ou a vulnerabilidade assimétrica em comparação com outros governos e às grandes organizações, surgem inúmeras oportunidades para que indivíduos e organizações criminosas possam agir usando dele a seu favor (MESQUITA, 2019).

> De 26 a 29 de novembro de 2008, dez membros fortemente armados do Lashkar-e-Taiba (LeT), um grupo separatista Kashmiri, atacaram vários locais públicos em Mumbai, Índia, com armas automáticas e granadas, matando 164 pessoas e ferindo 300. Este foi um dos primeiros casos conhecidos de terroristas empregando poderosos algoritmos de busca como o Twitter ou a análise de links usada no sistema PageRank do Google, o que permitiu aos membros do LeT acessar informações de enormes pools de dados em tempo real. Durante os ataques, um centro de operações do LeT baseado no Paquistão comunicou-se com os terroristas via telefones da Internet para fornecer-lhes inteligência de código aberto (OSINT). A partir do centro de operações, os membros do LeT mineravam a Internet e a mídia social, explorando o poder dos *Big Data* para fornecer aos atacantes uma vantagem de inteligência sobre as agências de policiamento indianas. Os atacantes foram, assim, mantidos atualizados sobre a situação da resposta do governo

> indiano e até receberam perfis pessoais dos reféns que capturaram no hotel Taj Mahal Palace (ZWITTER, 2015, p. 1, tradução do autor).

Acredita-se também que a soberania dos Estados começa a ser desafiada ao passo em que os mesmos se tornam grandes alvos para qualquer indivíduo ou organização com motivações ideológicas ou financeiras, conforme governos passam a depender mais e mais de sistemas e infraestruturas críticas ligadas pela internet das coisas. Instituições financeiras, indústrias petrolíferas, instalações de energia nuclear, redes de energia elétrica e estruturas de comunicação são apenas alguns exemplos dessas vulnerabilidades (NYE, 2010 apud MESQUITA, 2019).

Consequentemente, estamos experimentando uma mudança do campo de batalha das ameaças tradicionais para espaços virtuais nos quais as ameaças são invisíveis. Como afirmaram Messias e Brandão (2013):

> A insegurança do ciberespaço transformou-se num mundo de rostos invisíveis, onde os hackers operam penetrando as fronteiras dos Estados. Para estes, o intuito de penetrar, explorar e abater os sistemas de segurança torna-se um desafio ou uma forma de exprimir a revolta contra algumas políticas, ou até mesmo um meio para denunciar infrações. Já o ciberterrorismo, ao contrário do *hacker*, tende a causar o maior número de danos irreparáveis nos sistemas informáticos, desde o sector estatal ao privado. Também operam na esfera da internet para a obtenção de fundos financeiros para levar a cabo as suas missões, com o roubo de dados financeiros dos cibernautas através das contas bancárias ou dos cartões de crédito (MESSIAS, BRANDÃO, 2013, p. 9).

Reardon e Choucri (2012) descrevem o ciberespaço como um novo "domínio" de conflito, um espaço de batalha no qual tanto Estados como atores não-estatais podem lançar ataques cibernéticos estratégicos contra adversários. Tal conflito pode ser totalmente contido dentro do ciberespaço, levar a uma escalada entre os combatentes no mundo físico, ou infligir danos econômicos ou físicos. Os autores argumentam que ataques estratégicos em larga escala através do ciberespaço contra infraestruturas críticas representam uma grave ameaça à segurança nacional. Tais problemas podem ser atraentes para um adversário, argumentam eles, porque podem ser baratos e difíceis de rastrear. O conceito foi projetado para ser um ambiente aberto, e tem uma arquitetura que permite um anonimato substancial, muitas vezes tornando difícil ou impossível atribuir um ataque a um determinado atacante com confiança (REARDON, CHOUCRI, 2012).

Por outro lado, uma nova realidade é imposta para os Estados nacionais pelo ciberespaço no que concerne às suas atividades de inteligência. Os governos internos

não têm mais o monopólio do controle sobre a informação e, além disso, seu papel é cada vez mais complicado pelo fato de que devem enfrentar outros atores que competem com eles em uma série de questões, até mesmo na regulamentação do próprio ambiente cibernético (MAIER, 2016).

Não somente, agora, multinacionais especializadas em tecnologia da informação e *Big Data* possuem acesso a meios para influenciar as ações e decisões de grupos ou indivíduos, mas cada vez mais surgem empresas privadas de segurança cibernética, especialistas em recuperação e análise de programas de espionagem. Essas empresas tornam o conteúdo de suas pesquisas público e o transmitem na mídia, promovendo o acesso de qualquer cidadão ao conhecimento sobre as ferramentas de espionagem cibernética que os Estados têm a sua disposição, enfraquecendo sua efetividade (NOCETTI, 2018 *apud* MESQUITA, 2019).

Messias e Brandão (2013) definem em seu trabalho cinco tipos de atividades capazes de ameaçar indivíduos, organizações e Estados através do mundo virtual. Todas variando em motivação, grau de domínio técnico, nível de profissionalismo ou associação criminosa. Sendo elas a desobediência civil eletrônica, o cibercrime, o hacktivismo, o ciberterrorismo e a ciberguerra (MESSIAS, BRANDÃO, 2013).

O que os autores se referem como desobediência civil eletrônica, utilizam para denominar o que é também conhecido como *hacking,* ou o ato ou o conjunto de ações, através de *softwares*, com o objetivo de explorar vulnerabilidades em sistemas de informática para ganhar acesso e controle sobre eles. A partir da década de 1990, com o advento do cibercrime, o termo ganhou uma conotação negativa, passando a englobar a ação de contornar barreiras de segurança para atingir um fim qualquer — ético ou não (MESSIAS, BRANDÃO, 2013).

O cibercrime, por sua vez, se refere a toda vez em que o domínio cibernético é utilizado para alcançar um objetivo criminoso ou quando o ciberespaço se torna alvo de uma infração. A lista de ações que constituem cibercrimes é longa e variada, incluindo interceptação ilegal de comunicações, roubo de propriedade intelectual, roubo de propriedade cibernética, lavagem de dinheiro, evasão fiscal eletrônica, vandalismo eletrônico que inclui ciberterrorismo, extorsão e sabotagem, fraude informática, falsificação de cartões, roubo de identidade, crimes de conteúdo ofensivo, espionagem eletrônica e uso não autorizado de um recurso informático (MESSIAS, BRANDÃO, 2013).

O ciberterrorismo em si se refere a um ataque ou a uma tentativa de ataque a uma rede de comunicações ou de computadores, com o objetivo de intimidar ou coagir um governo ou seu pessoal a atingir fins políticos ou sociais. Além disso, a ameaça deve resultar em violência contra pessoas ou bens, ou pelo menos causar danos suficientes para causar medo. Ataques que resultem em morte ou danos físicos, explosões, acidentes aéreos, contaminação da água ou graves perdas econômicas são alguns exemplos. Entretanto, o ciberterrorismo pode incluir também o uso do mundo cibernético por organizações terroristas para coletar informações, angariar fundos ou difundir propaganda (MESSIAS, BRANDÃO, 2013).

Como exemplo de organizações que praticam do ciberterrorismo, podemos citar, a partir do relatório do Diretor Nacional de Inteligência dos EUA para um comitê do Senado norte-americano chamado *Foreign Cyber Threats to the United States*, a Al-Qaeda, o Hezbollah, o Hamas e o próprio Estado Islâmico que, apesar de ainda não possuírem conhecimento ou recursos suficientes para atingirem infraestruturas críticas diretamente através do ciberespaço, utilizam do domínio cibernético para coletar informações de inteligência, coordenar operações, arrecadar fundos, disseminar propaganda e incitar novas ações (MESQUITA, 2019).

É importante distinguirmos entre o ciberterrorista e o cibercriminoso. Enquanto o primeiro é impulsionado por causas ideológicas, sociais ou políticas, o cibercriminoso possui objetivos meramente econômicos, procurando apenas o enriquecimento através de atividades criminais no espaço cibernético (RAGOT, 2015 *apud* MESQUITA, 2019).

Os autores definem a ciberguerra como o conjunto de ações que visam preservar a integridade de sistemas de informação, impedindo sua exploração, corrupção ou destruição por adversários e, simultaneamente, executar ações que permitam a exploração, corrupção ou destruição dos sistemas de informação dos adversários, obtendo assim vantagem informativa, na esfera política, econômica ou militar. O conceito é comumente utilizado para definir conflitos entre Estados e devido a isso vamos falar mais sobre ela no terceiro capítulo (MESSIAS, BRANDÃO, 2013).

Por fim, o hacktivismo, diferente do *hacking,* é o reflexo do ativismo tradicional no mundo real para o virtual com o objetivo de atrair a atenção da opinião pública, de um setor da sociedade ou da classe política para uma causa política ou social. É consenso que o hacktivismo é mais bem definido como o uso não violento de

ferramentas digitais ilegais ou ferramentas de legalidade duvidosa para fins políticos (MESSIAS, BRANDÃO, 2013).

Como exemplo de organizações hacktivistas podemos considerar grupos reconhecidos como o *Anonymous* ou o *WikiLeaks*. Um exemplo de ação cometida por esses grupos que podemos citar são ataques DDos, ataques de negação de serviço distribuído, e constituem em bombardear sites ou programas com milhares de requisições virtuais por segundo, impedindo totalmente o funcionamento do recurso, o que pode ser usado para incapacitar sites oficiais de órgãos políticos ou de empresas. Um outro exemplo é o de *web defacement*, quando um hacktivista invade uma página na internet e altera o *layout* do site para demonstrar uma mensagem conforme sua causa ou objetivo (MESSIAS, BRANDÃO, 2013).

Um ponto chave a se entender sobre cada um dos atores responsáveis pelas atividades acima mencionadas é que estes em muitos casos podem ser usados como e se encaixar no conceito de *Proxies*. Os atores *Proxies* atuariam sob demanda, trabalhando para atingir os objetivos de terceiros que os contratassem com tal fim. Indivíduos, redes hacktivistas, redes de cibercriminosos ou até mesmo empresas de segurança privada podem agir como *Proxies* para os interesses de outros atores que queiram permanecer em segredo. Um ator acusado muitas vezes por supostamente utilizar tal ferramenta é a Rússia, que veremos mais a fundo no terceiro capítulo (NOCETTI, 2018 *apud* MESQUITA, 2019).

Como podemos observar a partir das diferentes atividades, são várias as ameaças que podem advir de indivíduos e organizações criminosas utilizando do mundo cibernético. Espionagem, crimes cibernéticos com o objetivo de roubo e extorsão de dinheiro ou dados, desestabilização através de mídias sociais e sites de informação e ataques no mundo digital com o objetivo de paralisar ou destruir a infraestrutura no mundo físico são apenas alguns exemplos (MESQUITA, 2019).

A Conferência de Segurança de Munique, em fevereiro de 2017, declarou que os ataques cibernéticos podem visar também o sistema político ocidental e os valores sobre os quais esse sistema é fundado (democracia representativa, separação de poderes, liberdade de expressão), o que leva a alguns autores a sugerir que a democracia e seus atributos devem ser tratados como uma infraestrutura crítica diante de ataques cibernéticos e manipulações da Internet (MUNICH SECURITY REPORT, 2017 *apud* MESQUITA, 2019).

De acordo com Valeriano e Maness (2018), a ameaça cibernética e a vulnerabilidade permanecem como uma prioridade na opinião pública. Segundo James Clapper, Diretor de Inteligência Nacional dos EUA, os ataques cibernéticos são uma ameaça significativamente maior à segurança nacional do que os extremistas sunitas, as ambições nucleares do Irã e da Coréia do Norte, e os agentes russos e chineses que procuram penetrar na segurança dos EUA (VALERIANO, MANESS, 2018).

Podemos citar e analisar uma série de casos em que ataques cibernéticos foram responsáveis por danos alarmantes a uma nação. É possível traçar um histórico de ataques e invasões virtuais até 1982 quando, acredita-se que, um sistema de gasodutos da União Soviética foi infectado propositalmente por uma bomba lógica, um código malicioso inserido em *softwares* que permanece inativo até que certa condição seja cumprida, executando sua função apenas após um determinado período ou uma mudança específica no sistema. A bomba lógica usada contra o gasoduto fez com que suas bombas e compressores começassem a funcionar em níveis perigosamente altos, o que ultimamente levou a uma explosão, na região da Sibéria, equivalente a um quinto da força de uma bomba atômica (BRONK, 2015).

Em 2007, a Estônia foi vítima de um ataque DDos generalizado que partiu de aproximadamente 85 mil computadores infectados e durou três semanas, tirando do ar os sites de todos os ministérios do governo estoniano, os serviços online de dois grandes bancos e até o servidor dos e-mails de parlamentares. O ataque foi atribuído a hacktivistas russos, em protesto à remoção de uma estátua que homenageia o Exército Vermelho, instalada durante o período da União Soviética. Este se tornou o primeiro ataque cibernético oficialmente reconhecido contra um Estado-Nação, visto que nunca foi possível comprovar oficialmente a causa das explosões em 1982, e chocou a comunidade internacional, alertando a todos a necessidade de prevenção contra este tipo de ameaça (RID, 2012 *apud* MESQUITA, 2019).

Em 2008, o Exército dos EUA sofreu um ataque cibernético massivo quando um vírus de computador, intitulado *Agent.btz*, invadiu a rede local de inteligência das operações do exército no Oriente Médio. O *Agent.btz* era um verme de computador auto-replicativo que foi capaz de se espalhar por toda a rede e permanecer indetectado por um longo período, coletando e enviando milhares de informações confidenciais para o criador do vírus. Mesmo após ter sido detectado, o Pentágono demorou ainda quatorze meses para conseguir remover o invasor de suas redes

militares — isso porque o vírus continuava sempre mutando, transformando sua assinatura, tornando impossível a detecção. Três anos após a declaração do Pentágono de que a ameaça havia sido eliminada, novos relatórios surgiram afirmando que o vírus ainda estava ativo no sistema sob novas variações (SHAHROM, MAAROP, SAMY, HASSAN, RAHIM, MAGALINGAM, KAMARUDDIN, 2021).

E o mais interessante é a forma como a invasão supostamente começou. Um membro das forças armadas dos EUA encontrou um flash drive USB no estacionamento de uma das instalações do Departamento de Defesa dos EUA no Oriente Médio e inseriu esse *pen drive* desconhecido em um laptop conectado ao Comando Central dos EUA, de onde conseguiu se espalhar e infectar todo o sistema. Este incidente ficou conhecido como a pior violação dos computadores militares dos EUA na história (SHAHROM, MAAROP, SAMY, HASSAN, RAHIM, MAGALINGAM, KAMARUDDIN, 2021).

Em 2010 ocorreu, provavelmente, um dos casos mais discutidos em trabalhos acadêmicos sobre o tópico de ataques cibernéticos, o vírus *Stuxnet*, que foi implantado e atacou a usina nuclear iraniana de Natanz, visando os computadores que controlavam as centrífugas e se espalhando até acessar o central do reator nuclear. Os atacantes conseguiram comprometer o trabalho do programa, afetaram o funcionamento dos computadores e levaram as centrífugas a se destruírem (NERADKO, 2018).

Assim como no caso do *Agent.btz*, o *Stuxnet* provavelmente conseguiu penetrar os sistemas da instalação por meio de um dispositivo USB que foi conectado a algum computador pertencente à rede interna da usina, e foi se reproduzindo e se espalhando pelo sistema. Ainda que o Irã não tenha revelado os números, é estimado que cerca de 984 centrífugas de enriquecimento de urânio foram inutilizadas, o que causou uma redução de 30% na produtividade do local e atrasou o programa nuclear iraniano em cerca de dois anos (BROAD; MARKOFF; SANGER, 2011 *apud* MESQUITA, 2019).

Citando a forma como o Secretário de Defesa dos Estados Unidos, Leon Panetta advertiu a população estadunidense, após o incidente com o vírus *Stuxnet*, sobre a possibilidade de um *Cyber Pearl Harbor*, Nye defendeu que um Cyber 11/9 seria muito mais provável. O autor fez tal afirmação considerando que o primeiro implica um ataque por parte de outro Estado, enquanto o segundo implica um ataque

vindo de um ator não estatal, o que em sua visão existem mais chances de ocorrer (NYE, 2012 *apud* MESQUITA, 2019).

Novos casos de ataques cibernéticos vêm aumentando e aparecendo incessantemente desde então. Como por exemplo, o conhecido caso do *ransomwares* (*malware* que restringe o acesso ao sistema infectado e cobra um resgate em criptomoedas para que o acesso possa ser restabelecido) *WannaCry* e *NotPetya*, ambos ocorrendo em um intervalo de dois meses durante o ano de 2017. O primeiro atingiu mais de 300 mil computadores, em 150 países, e tinha como alvos principais empresas e certas infraestruturas críticas de alguns países. Estima-se que o vírus tenha causado um prejuízo entre quatro e oito bilhões de dólares, sem contar que ele chegou a atingir inúmeros hospitais no Reino Unido, pondo em risco a vida de centenas de pacientes (GREENBERG, 2018 *apud* MESQUITA, 2019).

O *NotPetya* foi desenvolvido em meio ao conflito entre Rússia e Ucrânia, que vinha se desenvolvendo desde 2014, por um grupo russo conhecido como *Sandworm* que lançou o *malware* contra o rival. Esse novo *ransomware* era extremamente agressivo, se propagando de forma extremamente rápida e inédita e, ainda que exigisse o pagamento de resgate nos computadores contaminados, qualquer pagamento era inútil, pois o computador já estava inutilizado, já que o vírus o danificava de modo irreversível. Após ter sido disparado na Ucrânia, ele rapidamente se espalhou de forma internacional. Muitas empresas multinacionais acabaram infectadas pelo programa, em todos os casos causando prejuízos da ordem de centenas de milhões de dólares (GREENBERG, 2018 *apud* MESQUITA, 2019).

Em um caso extremamente recente, a companhia Colonial Pipeline foi atacada por um *ransomware* no dia seis de maio de 2021, permitindo que criminosos cibernéticos penetrassem em todo o sistema de gasoduto da empresa, com implicações econômicas significativas para toda a costa leste dos EUA. Especialistas em segurança consideram o ataque à empresa um importante alerta e um momento equivalente a *Pearl Harbor* para a segurança cibernética. Relatou-se pânico, desorganização social e uma falta paralisante de combustível seguindo os ataques (REEDER, 2021).

Estes vários eventos apresentam uma imagem clara da grande capacidade dos ataques cibernéticos para ajudar cibercriminosos, ciberterroristas ou hacktivistas a atingir seus objetivos e danificar seus alvos de forma severa. Além desta capacidade, há uma grande variedade de diferentes abordagens que podem ser utilizadas, bem

como uma grande variedade de tipos de ataques que são possíveis. Paralelo a isso, devemos ressaltar que as situações descritas são as que conhecemos até o momento, e não um quadro fixo e imutável. Com os rápidos desenvolvimentos tecnológicos da sociedade atual, temos agora acesso a ataques com características devastadoras que eram inimagináveis mesmo há apenas alguns anos (MESQUITA, 2019).

A partir disso, podemos perceber realmente quanto às ameaças cibernéticas deixaram de ser hipóteses e previsões e se tornaram casos reais, cada vez mais frequentes. Conforme Estados passam a se beneficiar cada vez mais de redes cibernéticas, cada vez mais eles se tornam vulneráveis aos tipos de ataques vistos anteriormente; e, cada vez mais, surgem oportunidades para indivíduos ou grupos com intenções maliciosas.

3.2 AS CORPORAÇÕES E O CIBERESPAÇO

Por mais assustador que todas as formas em que o Estado se tornou vulnerável a ataques advindos do ciberespaço possa parecer, é interessante observarmos também como as nações perdem poder frente a guerra da informação. Empresas de tecnologia agora possuem o poder para controlar enormes fluxos de informação e, portanto, manipular a seu favor a opinião pública.

Os atores privados agora veem o ambiente digital e os dados que circulam dentro dele como essencial em seu poder político e econômico. Cada vez mais, os mercados passaram a ver a coleta maciça de dados como um elemento-chave de seu progresso e desenvolvimento. Através da computação, praticamente todos os aspectos da vida humana se tornaram matéria-prima para um novo mercado baseado na venda de previsões de comportamento dos consumidores (ASSIS, 2020).

> Essa nova lógica de acumulação de capital, baseada na monetização de dados comportamentais, foi definida pela autora Shoshana Zuboff (2014) como capitalismo de vigilância, uma variante extrativa do capitalismo de informação, responsável por direcionar o setor privado rumo a um projeto de vigilância lucrativo, transformando os dados na mais nova e lucrativa commodity comercial do século XXI (ZUBOFF,2019). Modelo de negócios também categorizado como capitalismo de dados (ZUBOFF, 2019 *apud* ASSIS, 2020, p. 22).

A capitalização da vida social ocorre através do registro de todas as nossas atividades digitais, como sites visitados, links clicados, passagem de mouse, curtidas no Facebook, páginas visualizadas, tempo de permanência e localização. Tais dados

são capazes de fornecer perfis de comportamento e preferências dos usuários, transformando qualquer dado em ouro ou, em outras palavras, convertendo toneladas de dados brutos em algoritmos altamente rentáveis (ASSIS, 2020).

Quanto mais nossas vidas se espelham em uma realidade cibernética e são gravadas, mais nosso presente e passado se tornam quase completamente transparentes para atores com as habilidades e o acesso certos. Dados compilados a partir de dados estatísticos e através do *Big Data* podem ser usados para influenciar o comportamento, por exemplo, através de *marketing* direcionado, fornecendo às pessoas as informações que elas desejam. Se você conhece as preferências e condições de um grupo específico você pode usar estas informações para dar incentivos para encorajar ou desencorajar certos comportamentos (ZWITTER, 2014).

Além disso, o ciberespaço permite outras técnicas, como os *bots* que se infiltram no Twitter para criar falsos debates populares sobre um partido político que o público humano também percebe falsamente como legítimo. Especula-se que um exemplo destes bots pode ter contribuído na decisão eleitoral entre Martha Coakley e Scott Brown nas eleições especiais de 2010 em Massachusetts para preencher a vaga no Senado americano. Acredita-se que o *bot* criou uma campanha de difamação no Twitter na forma de um falso debate público favorecendo a vitória de Brown (ZEIFMAN, 2013 *apud* ZWITTER, 2014).

Um dos exemplos mais bem documentados de empresas privadas utilizando do *Big Data* para manipular a opinião popular que podemos citar é certamente o caso da *Cambridge Analytica* e do *SCL Group*. Fundado por Nigel Oakes em 1993 e desenvolvido em conjunto com o *Behavioural Dynamics Institute* (BDI), um centro de pesquisa para comunicação estratégica, o *Strategic Communication Laboratories* (SCL) nasceu para o estudo do comportamento de massa e como mudá-lo (PRIVACIDADE, 2019).

Após uma expansão comercial bem-sucedida, a SCL entrou nas arenas militares e políticas. A empresa, primeiro, passou a trabalhar usando recursos para influenciar o comportamento da conduta inimiga em países como o Iraque e o Afeganistão e, após, começou a trabalhar com campanhas de desinformação militar para o *branding* das mídias sociais e para o direcionamento de eleitores. Como expositora na *Defense and Security Equipment International* (DSEI), a maior feira de tecnologia militar do Reino Unido, em 2005, a SCL demonstrou sua capacidade de conduzir operações de influência orquestrando manipulação em massa sobre o

público de uma cidade como Londres, participando de mais de 25 campanhas políticas internacionais e campanhas eleitorais desde 1994, de acordo com seu website (PRIVACIDADE, 2019).

A SCL tem se envolvido principalmente na política de países em desenvolvimento, onde tem sido utilizada pelos militares e políticos para estudar e manipular a opinião pública. A empresa usa a psicografia para fornecer uma visão do pensamento do público-alvo. Usando essas técnicas, a SCL alegou ser capaz de fomentar golpes de Estado. De acordo com seu site, a companhia influenciou eleições na Itália, Letônia, Ucrânia, Albânia, Romênia, África do Sul, Nigéria, Quênia, Maurício, Índia, Indonésia, Filipinas, Tailândia, Taiwan, Colômbia, Antígua, São Vicente e Granadinas, São Cristóvão e Nevis e Trinidad e Tobago. Entre outros, afirma que sua metodologia foi aprovada ou endossada por agências do governo do Reino Unido e do governo dos EUA (PRIVACIDADE, 2019).

Em 2010, a empresa foi capaz de favorecer e garantir a eleição de um dos partidos concorrentes durante as eleições gerais de Trinidad e Tobago, mudando o rumo do país caribenho ao impulsionar um movimento de desinteresse e resistência ao voto na juventude caribenha do país. O movimento *Do so*![2], orquestrado pela SCL, mirava a opinião de adolescentes e jovens adultos do país incentivando resistência contra políticos e as eleições em geral, desincentivando o voto. O partido Congresso Nacional Unido, o qual era cliente do *SCL Group*, de maioria indiana, levou vantagem a partir disso porque enquanto os jovens indianos eram obrigados pelos pais a votar, os jovens afro-caribenhos se recusaram, o que gerou uma diferença de 6% dos votos, o suficiente para vencer uma disputa acirrada (PRIVACIDADE, 2019).

Em 2013, foi fundada uma subsidiária do *SCL Group* especializada somente em campanhas eleitorais, a *Cambridge Analytica*. Desde sua fundação, a organização agiu sobre dezenas de eleições em diversos países diferentes, mas os dois casos mais marcantes e que ultimamente levaram ao seu fim foram os casos do Brexit e das eleições presidenciais dos EUA de 2016. No primeiro, a companhia negou envolvimento com a campanha *Leave.EU*. Entretanto, além de uma série de evidências apontando o contrário, Brittany Kaiser, uma antiga funcionária que depôs contra a empresa, afirmou a utilização de tecnologias de comunicação classificadas

[2] Faça-o!

como de nível militar pelo governo britânico durante o movimento do Brexit (PRIVACIDADE, 2019).

Em contrapartida, a empresa admitiu trabalhar nas eleições presidenciais estadunidenses de 2016. Desde 2014, a *Cambridge Analytica* vinha coletando dados pessoais de usuários da internet, que sem o seu total conhecimento, preenchiam questionários de personalidade que arquivavam todas as suas respostas e construíam um perfil da pessoa a partir de cada ponto de dado obtido. Esses dados incluíam todo o tipo de característica da pessoa, seus interesses, seus comportamentos, seu cronograma e milhares de outras informações pessoais. A firma admitiu, posteriormente, ter coletado em média cinco mil pontos de dados para cada um de 230 milhões de eleitores americanos (PRIVACIDADE, 2019).

A CA começou a utilizar então estes dados a seu favor durante as eleições primárias de 2015, trabalhando para a campanha do candidato Ted Cruz, o que lhe concedeu uma vantagem significativa sobre seus rivais. Após Donald Trump receber a indicação como o candidato republicano na disputa final, a empresa fechou um contrato para trabalhar na campanha do futuro presidente (PRIVACIDADE, 2019).

O antigo CEO[3] da empresa, Alexander Nix, afirmou que, na época em que a CA fechou o contrato, a campanha de Trump era muito pequena e não tinha infraestrutura. A partir disso, a empresa conseguiu arrecadar 27 milhões de dólares em fundos para a campanha e assumiu controle de toda a parte de análise de dados, pesquisa, TV e tratamento de doações (BUTCHER, 2017).

Utilizando de *Big Data* e psicográficos, a partir dos milhares de dados coletados das pessoas, a *Cambridge Analytica* era capaz de bombardear usuários de redes sociais com vídeos digitais com conteúdo de alta precisão. Além disso, a empresa visava sempre o eleitor que ela havia denominado como persuasivo, aquele que ainda não havia se decidido sobre quem votar, e sempre visava os eleitores influenciáveis de estados decisivos dentro do país como Michigan, Wisconsin, Pensilvânia, Flórida, entre outros. A campanha criava, então, anúncios personalizados para atingir esses indivíduos e mudar a maneira como eles enxergam o mundo. O diretor da campanha de Trump em 2016 alegou ter promovido 5,9 milhões de anúncios visuais durante a campanha, enquanto a campanha da oponente, Hillary Clinton, promoveu apenas 66 mil (PRIVACIDADE, 2019).

[3] Pessoa com maior autoridade na hierarquia operacional de uma organização.

Após múltiplos antigos funcionários terem se pronunciado publicamente contra a empresa, uma série de investigações por parte do governo dos EUA e do Reino Unido e uma ação judicial emitida por David Carrol, um professor de mídia de Nova York, em primeiro de maio de 2018, o Grupo SCL, junto com a *Cambridge Analytica*, declarou que fecharia as operações. O grupo foi liquidado e comprado pela *Emerdata Limited* (PRIVACIDADE, 2019).

Carole Cadwalladr, repórter e redatora para o jornal britânico *The Observer* e uma das primeiras jornalistas a escrever sobre a relação entre a *Cambridge Analytica* e as eleições, afirmou que o uso das redes sociais como uma forma de manipular a população representa uma clara ameaça para a integridade da democracia e da soberania nacional. Ela se questiona se algum dia será possível termos uma eleição livre e justa na era do *Big Data* (PRIVACIDADE, 2019).

> A ascensão de *Big Data* também apresenta outros desafios epistêmicos, fundamentais. Os marcos morais e legais pioneiros durante o Iluminismo e codificados na era pós-guerra são, como os direitos humanos, inerentemente concebidos em torno do ator individual e seus interesses individualistas específicos, como a privacidade. Estas normas, entretanto, não são adequadas quando se trata da privacidade de grupos. Muitos também levantam preocupações de que este foco em grupos e comportamento grupal possa levar à caracterização racial, especificamente no contexto do policiamento preditivo (ZWITTER, 2015, p. 12, tradução do autor).

A grande maioria dos dados coletados pela *Cambridge Analytica* foram obtidos a partir do Facebook que, junto de outras organizações como o Google, é responsável por coletar o maior volume de informações e dados de pessoas na internet. Existe pouco controle e conhecimento sobre o que essas empresas fazem com estes pacotes massivos de dados, além de vendê-los à varejistas online. E, apesar de Mark Zuckerberg, dono da corporação, ter deposto frente ao Senado americano se desculpando ao público e a empresa ter pagado uma multa financeira simbólica, o Facebook ainda consegue atuar sobre dados pessoais de seus milhões de usuários de forma praticamente irrestrita (PRIVACIDADE, 2019).

Grande parte de legislações sobre o ciberespaço em países ao redor do mundo foram pensadas e redigidas há mais de vinte anos, quando a internet não comportava uma fração do público e do fluxo de informações que hoje ela suporta. O público em geral não compreende suficientemente bem o fenômeno do *Big Data* para estar particularmente preocupado com ele, ou para exigir de seu governo proteções específicas contra suas implicações. Há vislumbres ocasionais da realidade do domínio cibernético fornecido pelos denunciantes e jornalistas investigativos.

Entretanto, isto ainda é insuficiente para que o público em geral reconheça sua pegada digital gerada pelo uso da Internet e do celular. Embora o "direito de ser esquecido" seja um conceito sensato em certos casos, aplicá-lo como um indivíduo a uma empresa de cada vez ainda deixa inalterados os muitos outros coletores e vendedores de dados que estão coletando as mesmas informações e de cujas atividades não estamos cientes (ZWITTER, 2015).

3.3 A AÇÃO DE ATORES NÃO-ESTATAIS NO CIBERESPAÇO E SUA INFLUÊNCIA SISTEMA INTERNACIONAL

A partir do que vimos ao longo deste capítulo, torna-se claro a ameaça que atores não-estatais podem se tornar para a soberania estatal através do ciberespaço. Seja em razão de ataques diretos a infraestruturas críticas ou em razão da manipulação da opinião popular, governos devem seriamente repensar sua abordagem para com a segurança cibernética. Não existe limite para a possibilidade de táticas diferentes que podem ser empregadas para se atingir um objetivo potencialmente malicioso através do mundo virtual.

Em uma entrevista para um repórter disfarçado, Alexander Nix revelou que a *Cambridge Analytica* além de usar de anúncios direcionados para dissuadir populações, usava armadilhas sexuais, falsas campanhas noticiosas e operações com ex-espiões para decidir campanhas eleitorais em todo o mundo. As táticas sujas incluíam capturar candidatos rivais em falsas operações de suborno e a contratação de prostitutas para seduzi-los (GRAHAM-HARRISON; CADWALLADR; OSBORNE, 2018).

A CA e o grupo SCL foram apenas a primeira organização descoberta por usar de psicográficos e *Big Data* para manipular populações. Mas elas com certeza não são as únicas, e o mercado para este tipo de tecnologia e conhecimento apenas tende a crescer. Um grupo ou empresa pequena ainda possui uma certa limitação de quantas pessoas ele pode alcançar. Porém, um gigante como a Google ou o Facebook possui a tecnologia e o orçamento para atingir o mundo inteiro e a capacidade de empregar qualquer técnica que bem entender.

Esta nova realidade desafia todas as pré-concepções de teorias clássicas sobre soberania estatal e tem o potencial para desestabilizar o SI. No domínio

cibernético, os atores encontram cada vez mais espaço para se orientarem livres das limitações impostas pelas legislações nacionais. A emergência de novos atores não-estatais com capacidades de agir fora dos limites fronteiriços gera inevitavelmente uma mudança na balança de poder do SI. O Estado deixa de ser o único agente relevante a partir da interdependência complexa.

4 O ESTADO NO CIBERESPAÇO E SUA INFLUÊNCIA NO SISTEMA INTERNACIONAL

Ao longo do próximo capítulo será discutido como, em contraste ao que foi apresentado no capítulo anterior, o Estado utiliza do ciberespaço como uma estratégia de guerra, implementando ferramentas digitais para obter vantagens no campo militar e político.

Será discutido, também, como tal fator é usado como uma ferramenta de controle social, explorando a forma como o governo norte-americano incentivou o desenvolvimento da internet como uma forma de expandir sua capacidade de vigilância. No presente capítulo, também é observado como Estados autoritários como China ou Coreia do Norte utilizam da censura e do controle digital como uma maneira de se proteger de influências estrangeiras e de manipular sua população.

Por último, será realizada uma recapitulação dos principais pontos debatidos. Trazendo uma reflexão sobre o impacto dessas considerações no SI.

4.1 O CIBERESPAÇO COMO ESTRATÉGIA DE GUERRA

Por mais sombria e desesperada que possa parecer a situação em relação a ameaça cibernética, especialmente considerando seus possíveis efeitos sobre a balança de poder internacional, é preciso entender que ao mesmo tempo em que o domínio cibernético surge como um novo campo de batalha, semelhante à área terrestre, marítima e aérea, e o Estado transforma-se em vulnerável a ataques advindos desse novo espaço, ele também torna-se capaz de utilizar do mesmo para seus próprios interesses e objetivos. De fato, os Estados obtiveram vantagens significativas com a emergência do ciberespaço, tanto no âmbito doméstico de suas políticas quanto no âmbito da política internacional (MESQUITA, 2019).

Apenas para exemplificar, estipula-se que praticamente todos os casos de ataques cibernéticos históricos, citados no capítulo três, tenham sido orquestrados por governos nacionais, operando através de *proxies*. Como foi mencionado anteriormente, suspeita-se que o governo russo faça uso constante de terceiros para desenvolver suas armas virtuais e para conduzir seus ataques (MESQUITA, 2019).

No caso do grande ataque cibernético ocorrido na Estônia, em 2007, acredita-se que o Kremlin tenha contribuído com o evento. Logo após os ataques DDos, o

governo estoniano foi rápido em acusar o governo russo como o responsável. Porém, uma série de investigações feitas por especialistas técnicos, tanto da Comissão Europeia quanto da OTAN, foram incapazes de encontrar evidências críveis de participação russa — e o Kremlin negou qualquer envolvimento. Um ano mais tarde, entretanto, um grupo juvenil pró-Putin, chamado *Nashi,* alegou ter orquestrado os ataques. A legitimidade da coletividade como movimento juvenil independente tem sido fortemente questionada, no entanto, pois fontes sugerem que o governo de Putin financia suas atividades. O relacionamento do grupo com as autoridades ecoa a ambiguidade que envolve o lugar de atores não-estatais em muitos reinos da guerra moderna (MUTI, TAJER, MACFAUL, 2014).

Em relação à invasão do Comando Central dos Estados Unidos, em 2008, o verme *agent.btz* pertence à mesma família de *spywares*[4] que o Cavalo de Tróia virtual, *Turla* — um spyware desenvolvido por um grupo de hackers que carregam o mesmo nome do programa. Tal *software* esconde a presença da operação de espionagem e cria um sistema de arquivo oculto e criptografado para armazenar dados roubados e ferramentas usadas pelos atacantes; roubo de senhas e documentos e pequenos programas para coleta de informações sobre o sistema e. Os operadores também podem baixar ferramentas especializadas em um sistema infectado, adicionando qualquer funcionalidade que queiram, incluindo-a no sistema de arquivo criptografado (APPS, FINKLE, 2014).

O grupo *Turla*, também conhecido como *Snake*, é um dos mais antigos grupos de *ciber* espionagem ainda ativos, com mais de uma década de experiência. Seus operadores se concentram principalmente em alvos de alto perfil, como governos e entidades diplomáticas na Europa, na Ásia Central e no Oriente Médio. Mais recentemente, vários países europeus, incluindo a França e a República Tcheca, denunciaram ataques do grupo contra seus governos. O *Turla* também está ligado a uma conhecida operação de espionagem cibernética global, denominada *Red October*, que visava redes diplomáticas, militares e de pesquisa nuclear (FAOU, 2020).

Apesar de ser impossível confirmar qualquer coisa até que Moscou assuma a responsabilidade, especialistas ainda acreditam que os membros por trás da organização são um grupo de espiões russos. Peritos em ataques cibernéticos

[4] *Malwares* desenvolvidos especificamente para espionagem.

patrocinados pelo Estado dizem que os hackers apoiados pelo governo russo são conhecidos por serem altamente disciplinados, hábeis em esconder seus rastros, extremamente eficazes em manter o controle de redes infectadas e seletivos na escolha de alvos. Essa provável conexão entre *Turla* e o governo russo, coloca o Kremlin como o principal suspeito por de trás das invasões de 2008, quando teria usado de *spyware* para obter acesso a milhares de arquivos confidenciais de segurança americana direto da fonte (APPS, FINKLE, 2014).

Entretanto, a Rússia certamente não é o único Estado a supostamente utilizar do ciberespaço como arma; trazendo, novamente, o caso dos gasodutos soviéticos em 1982, acredita-se que a Agência Central de Inteligência (CIA) e o Escritório Federal de Investigação (FBI) dos EUA tenham sido os responsáveis por instalar a bomba lógica dentro dos computadores soviéticos. Como parte de uma operação de contrainteligência, as agências forneceram, para espiões da KGB[5] desavisados, chips de computador adulterados, turbinas defeituosas que foram instaladas em um gasoduto e planos incorretos que interromperam a produção de fábricas de produtos químicos e de uma fábrica de tratores (BRONK, 2015).

No caso do *Stuxnet*, apesar de nenhum país ter admitido qualquer envolvimento, devido à complexidade do vírus e ao fato de que a retardação do programa nuclear iraniano se alinha perfeitamente com os objetivos de Israel e dos EUA, muitos acusam estes dois Estados de terem desenvolvido o programa e coordenado o ataque. Em um artigo para o *The New York Times*, de 2012, escrito com base em extensas entrevistas com funcionários israelenses e americanos anônimos, David Sanger alegou que o ataque foi ordenado e desenvolvido conjuntamente pelos dois países em uma operação denominada de Jogos Olímpicos pela Administração Nacional de Segurança dos EUA (NSA). A operação foi uma empreitada de custo elevado, sendo planejada desde 2006, e representou um nível inédito de sofisticação técnica e de precisão operacional (MUTI, TAJER, MACFAUL, 2014).

Além dos acontecimentos previamente comentados, existem três outros casos paradigmáticos para o estudo da segurança cibernética que devemos observar. Primeiramente, durante sua intervenção na Guerra do Kosovo contra a República Federal da Iugoslávia em 1999, a Organização do Tratado do Atlântico Norte (OTAN) utilizou de instrumentos de guerra de informação em combate, como propagandas,

[5] Principal organização de serviços secretos da União Soviética que desempenhou as suas funções entre 13 de março de 1954 e 6 de novembro de 1991

campanhas de desinformação pela mídia, ataques DDoS, ataques a websites iugoslavos e, ainda, invasão das contas bancárias do líder iugoslavo Slobodan Milosevic. Isso marcou o primeiro uso sustentado do espectro completo dos componentes da guerra de informação em combate (CAVELTY,2010 *apud* MESQUITA, 2019).

Em outra ocasião, em setembro de 2007, durante a Operação Pomar, Israel utilizou de um ataque cibernético para desativar as posições de defesa aérea silenciosamente e permitir que os aviões israelenses entrassem no espaço aéreo sírio sem serem perturbados. A partir disso, Israel realizou um ataque aéreo contra uma instalação síria escondida longe das principais cidades do país, a 140 km da fronteira iraquiana. A instalação, chamada *Al-Kibar*, foi alegadamente um reator nuclear construído secretamente com a ajuda da República Popular Democrática da Coréia para a produção de plutônio. Os aviões israelenses foram capazes de adentrar o país inimigo sem nenhuma resistência por parte das defesas antiaéreas sírias (MUTI, TAJER, MACFAUL, 2014).

Um ano após os ataques israelenses, durante a guerra entre Rússia e Geórgia, que surgiu depois que a região georgiana da Abecásia e da Ossétia do Sul anunciaram sua secessão, a Federação Russa utilizou de uma série de ataques cibernéticos de baixo nível em conjunto com operações terrestres contra a República da Geórgia. Os ataques virtuais de baixa complexidade haviam começado aproximadamente uma semana antes do início do confronto militar, mas a onda de ataques cibernéticos atingiu em força total no mesmo dia em que a principal ofensiva militar começou com seriedade. Como na invasão contra a Estônia em 2007, mencionada na seção anterior, a ofensiva consistiu, principalmente, na desfiguração de *websites* e na interrupção de serviços baseados na *web*, atingindo bancos, entidades do setor privado e websites governamentais. Neste caso, novamente, o governo russo alegou que esses ciberataques eram uma atitude popular e estavam fora do controle do Kremlin. Entretanto, investigações mostraram, posteriormente, que os sites usados para lançar os ataques eram conectados ao aparato de inteligência russa (MUTI, TAJER, MACFAUL, 2014).

Pensando em um futuro não tão distante, Dunlap Junior (2014) argumenta que *Big Data* e as ferramentas para analisá-lo também apresentam uma oportunidade real para que os governos utilizem tecnologias de pronto alcance para melhorar sua capacidade de combate. Uma oportunidade seria a construção de bancos de dados

de potenciais oponentes militares que poderiam ser tão detalhados a ponto de incluir dossiês eletrônicos de membros individuais. Este tipo de informação, junto com outros dados e tecnologias, poderia ser explorada durante os conflitos para personalizar os meios e métodos de guerra até um grau totalmente novo, criando, segundo o autor, uma guerra hiper personalizada (DUNLAP JUNIOR, 2014).

Considerando o destaque significativo nos últimos anos da utilização de aeronaves pilotadas remotamente, também conhecidas como "drones", o exército dos EUA está desenvolvendo uma nova geração de pequenas máquinas capazes de operar em grupos em rede, ou "enxames". Outros relatos sugerem também o desenvolvimento de microdrones letais que se assemelham a insetos, com capacidade para se aglomerar através de becos, rastejar através de soleiras de janelas e empoleirar-se em linhas de energia elétrica enquanto procuram seu alvo. Paralelamente ao rápido desenvolvimento da tecnologia dos drones está o rápido avanço de *softwares* de reconhecimento facial (DUNLAP JUNIOR, 2014).

As forças armadas americanas poderiam então lançar enxames de drones equipados com *software* de reconhecimento facial para vasculhar os campos de batalha à procura de membros muito específicos da força inimiga. Estes poderiam ser oficiais, mas também técnicos selecionados e líderes de batalha que possuíam habilidades vitais e difíceis de substituir (DUNLAP JUNIOR, 2014).

O que tornaria esta estratégia extremamente efetiva não seria apenas sua capacidade de aleijar exércitos ao eliminar líderes ou estrategistas, mas também o efeito psicológico que causaria sobre cada membro da força inimiga. Um dos pilares que sustenta os soldados durante o conflito é seu relacionamento com os outros em sua unidade — este processo de união fornece um escudo contra o isolamento psicológico do campo de batalha. Isso muda com a guerra hiper personalizada ao visar abertamente determinados indivíduos; líderes, técnicos e especialistas se colocam sob um risco muito maior do que outros (DUNLAP JUNIOR, 2014).

Além disso, a pessoa perde sua habilidade de negação para lidar com o estresse do combate. Sabendo que o adversário possui a habilidade de personalizar a ameaça, e talvez até comunicá-la diretamente, é impossível argumentar a si próprio de que não se torna vítima da situação (DUNLAP JUNIOR, 2014).

> A noção de contato em larga escala — ainda que pessoal — com indivíduos de uma força oposta não é sem precedentes. Na verdade, uma versão inicial da hiper personalização da guerra ocorreu antes do início da guerra contra o Iraque, em 2003. As forças dos EUA enviaram milhares de e-mails pessoais para 'oficiais militares iraquianos advertindo-os a abandonar suas posições e

> veículos para não sofrerem danos' (DUNLAP JUNIOR, 2014, p.112, tradução do autor).

Novamente, olhando através destes múltiplos casos apresentados ocorridos nos primeiros vinte anos do século XXI e que ainda podem ocorrer no futuro, podemos perceber a grande capacidade que os ataques cibernéticos têm para auxiliar os Estados a atingir seus objetivos e, também, para impor graves prejuízos às vítimas. Além da capacidade do sistema, a variedade de diferentes abordagens que podem ser tomadas é surpreendente, bem como a gama de tipos de ataques que podem ser cometidos (MESQUITA, 2019).

Entretanto, um número cada vez maior de acadêmicos questiona a real possibilidade de uma guerra cibernética algum dia acontecer, e o quanto ataques cibernéticos realmente representam uma ameaça para um Estado. Em primeiro lugar, apesar de que indivíduos e grupos criminosos possam lançar ataques virtuais contra infraestruturas críticas e pessoas públicas, o que realmente pode causar danos significativos e a perda de vida humana, eles não possuem nenhuma forma de garantir que os danos infligidos se traduzam em uma mudança duradoura no equilíbrio de poder nacional (GARTZKE, 2013 *apud* MESQUITA, 2019).

Mesmo que ataques digitais sejam ameaças sérias e reais, sendo invasões para as quais a grande maioria das nações ainda não sabem como se defender, é muito mais difícil para um atacante descobrir como se beneficiar da agressão na Internet, a menos que os ataques cibernéticos ocorram em conjunto com ataques em outros domínios. Justamente em razão disso, o Estado continua sendo o único ator no SI com capacidade e conhecimento para efetuar uma ciberguerra (GARTZKE, 2013 apud MESQUITA, 2019).

A visão popular e o debate em torno do domínio cibernético foi fortemente moldado por descrições exacerbadas por parte de mídias em geral, sempre enfatizando a ideia da utilização de um ataque cibernético por um grupo terrorista para destruir infraestruturas críticas causando centenas de mortos. Como, por exemplo, derrubando um avião ou invadindo uma usina nuclear. Porém, muitos autores possuem uma visão mais pragmática sobre um possível ciber 11/9 (MUTI, TAJER, MACFAUL, 2014).

Tomemos como exemplo novamente o *Stuxnet*, o, até hoje, único ciberataque confirmado que danificou fisicamente uma infraestrutura crítica. O ator responsável pelo ataque teve que descobrir qual sistema de controle industrial era usado nas

instalações de enriquecimento de urânio, e o software que era usado para operá-lo. Além disso, a equipe teve de adquirir informações sobre as próprias centrífugas de enriquecimento e descobrir a que velocidade as girar para maximizar os danos estruturais. Mesmo antes disso, tiveram de descobrir como a instalação operava, inclusive como fazer com que seu software malicioso infectasse as máquinas certas — sem estas bases, o ataque não teria sido possível. O Stuxnet aconteceu apenas através da cooperação entre Israel e EUA em um projeto que levou quatro anos para ser realizado, com um nível de sofisticação que nenhuma organização criminosa é capaz de se comparar (MUTI, TAJER, MACFAUL, 2014).

O próprio Estado, contudo, pode muitas vezes não ter capacidade ou interesse de aliar seu poder bélico a uma estratégia que envolva o domínio cibernético. O *New York Times* relatou que antes das operações na Líbia em 2010, os EUA consideraram o emprego de metodologias cibernéticas contra os militares de Kadhafi, mas acabaram por rejeitá-las em parte devido à enorme dificuldade em fazê-lo (DUNLAP JUNIOR, 2014).

É preciso reconhecer a distinção entre o que é possível e o que é provável; devido às limitações da arma e as potenciais consequências de ação, é improvável que um estado lance uma operação cibernética maciça — mesmo contra um inimigo. Apesar de terem capacidades cibernéticas, Estados como os EUA e a Rússia se abstiveram de conduzir operações cibernéticas ofensivas em grandes conflitos como na Ucrânia, Líbia, Síria, Iraque e Afeganistão (VALERIANO, MANNESS, 2018).

Outrossim, de todos os ataques cibernéticos observados anteriormente, nenhum trouxe consequências desastrosas e duradouras para a soberania de qualquer um dos Estados mencionados. Os ataques cibernéticos contra a Estônia e a Geórgia causaram uma perturbação de alta visibilidade, mas tiveram pouco impacto a longo prazo e seus efeitos foram insignificantes. E o próprio caso do *Stuxnet*, apesar de ter retardado o programa nuclear iraniano, não foi o seu fim. A maioria dos incidentes cibernéticos que fazem as notícias ou que podem afetar nossa vida diária não afetam a soberania de uma nação (MUTI, TAJER, MACFAUL, 2014).

Estados hesitam em utilizar de ataques cibernéticos com fins destrutivos pois — uma invasão virtual que se comparasse a uma ofensiva militar poderia elicitar uma retaliação proporcional e, na sequência de tal ataque, as barreiras técnicas para obter certas provas da origem do ataque poderiam ser superadas pela vontade política de

responder a um ato de agressão. Sendo assim, o ataque perderia uma das qualidades que o definem, a dificuldade de atribuição (MUTI, TAJER, MACFAUL, 2014).

Como demonstra o caso da Operação Pomar, ataques cibernéticos podem ser melhor usados para diminuir a necessidade de danos colaterais desnecessários. Caso Israel não tivesse desabilitado digitalmente as armas antiaéreas Sírias, o ataque poderia ter gerado maior destruição e perda de vida humana para ambos os lados. Por enquanto, apesar das capacidades potencialmente destrutivas dos ataques cibernéticos, a flexibilidade que eles oferecem permite que ataques mortais sejam extremamente improváveis (MUTI, TAJER, MACFAUL, 2014).

Uma ciberguerra total e declarada, então, por mais devastadora e inevitável que possa parecer através da visão popular, ainda é simplesmente muito complicada e imprática para ser utilizada convencionalmente. O que é possível e utilizado com cada vez mais frequência, entretanto, é o ciberespaço como maneira de auxiliar estratégias consolidadas em uma guerra tradicional. Apesar de não revolucionar a maneira de se fazer guerra, a implementação de tecnologias cibernéticas no campo de combate, com certeza, dará significativas vantagens para quem as possuir.

4.2 O CIBERESPAÇO COMO CONTROLE SOCIAL

Entretanto, os impactos do mundo cibernético na vida civil não se limitam a sabotagem em larga escala ou terrorismo. Na realidade, a vigilância extensiva tornou-se o que a maioria das pessoas no mundo agora enfrenta. A revelação da ampla rede de vigilância, trazida por Edward Snowden e pelos arquivos da Administração Nacional de Segurança, vazados por ele para a imprensa, foi um choque considerável para a maioria dos civis, expondo a quantidade de privacidade que a maioria das pessoas perde assim que entram na internet (MUTI, TAJER, MACFAUL, 2014).

Mesmo que o Estado possa se sentir ameaçado pela nova Guerra de Informação, conforme visto no capítulo três, ele também é capaz de se beneficiar, e muito, pelo capitalismo de vigilância. Um dos exemplos mais conhecidos é certamente o dos EUA que, após a era Clinton e o estouro da bolha das empresas ponto.com, através de suas agências de inteligência começou a investir pesadamente nas empresas do Vale do Silício responsáveis pelo desenvolvimento de inovações na área de TI (ASSIS, 2020).

A CIA criou a In-Q-Tel, uma empresa de capital de risco, para investir em *startups* alinhadas com as necessidades de inteligência da agência. Dados demonstram que a companhia investiu ao todo em mais de 180 empresas do ramo de tecnologia. A In-Q-Tel podia agir de maneira independente sem a necessidade de aprovação da CIA e investir o dinheiro da forma como achasse melhor (ASSIS, 2020).

> [...] Dois critérios guiavam os investimentos realizados pela In-Q-Tel, estes deveriam trabalhar de maneira não classificada e as tecnologias deveriam ter potencial econômico, seguindo a política iniciada durante o governo Clinton. As principais áreas de investimento eram segurança da informação, uso da Internet, arquiteturas de distribuição como métodos para interagir com sistemas personalizados, mecanismos para permitir que aplicativos diferentes interajam, manipulação automática de dados arquivados e conectividade em ampla variedade de ambientes e, por fim, geração de conhecimento como tecnologia de mineração de dados. (ASSIS, 2020, p. 36)

A criação da In-Q-Tel, junto de outras iniciativas do governo americano, demonstrava uma mudança de posicionamento para com o setor privado. O sucesso do empreendimento da CIA inspirou outras agências governamentais a explorar e promover pesquisas através de capitais de risco. A partir disso, entende-se que teve início o complexo industrial informacional, a interseção do capital e do Estado na promoção do surgimento e crescimento de tecnologias voltadas à captação, armazenamento e processamento de informação (ASSIS, 2020).

Com os ataques do 11 de setembro e o lançamento da Guerra ao Terror em 2001, teve início, então, a era da vigilância e da ciber vigilância nos EUA. O discurso de securitização gerou um estado de exceção jurídico que restringiu direitos fundamentais de cidadãos norte-americanos, conferindo legalidade para uma vigilância sistemática que entorpecia o direito à privacidade da população (ASSIS, 2020).

Para combater o terrorismo, o governo americano desenvolveu uma necessidade crescente de captação de toda e qualquer informação disponível com a maior rapidez possível. Através disso, surgiu a legislação *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*, também conhecida como *Patriot Act* (ASSIS, 2020).

O *Patriot Act* representa um conjunto de leis que aumentaram o poder de ação de agências federais e de órgãos de inteligência dos EUA em relação à investigação e à vigilância de atores estrangeiros e nacionais. As agências, agora, podem coletar informações de cidadãos americanos e não-americanos sem precisar da instituição

de um julgamento de pertinência ou de um mandato. O *Patriot Act* também impactava a privacidade no ciberespaço, criando programas que posteriormente seriam expostos por Edward Snowden como exemplos de vigilância indiscriminada, como o PRISM (ASSIS, 2020).

O PRISM envolve a obtenção de informações pessoais por meio de empresas privadas que regularmente coletam grandes quantidades de dados pessoais para fins comerciais. Segundo Snowden, o programa é executado a partir da colaboração com uma série de empresas de serviços de internet como Microsoft, Google, Yahoo, Facebook, Paltalk, YouTube, Skype, AOL, Apple e empresas de telecomunicações, como BT, Vodafone Cable, Verizon Business, Global Crossing, Viatel e Interoute. O PRISM coletava dados que posteriormente seriam analisados e armazenados através de outros programas de vigilância voltados para a mineração de dados (ASSIS, 2020).

Além disso, o *Protect America Act* de 2007, entre outras medidas, permitia a cooperação entre empresas e o governo, fornecendo informações ou assistência sem a necessidade de alertar seus clientes. Logo após, em 2008, surgiu a FAA como um novo conjunto de emendas para a *Foreign Intelligence Surveillance Act* (FISA), lei federal que estabelece os procedimentos para a vigilância física e eletrônica praticada pelo governo norte-americano durante o processo de coleta de informações de governos e agentes de poder estrangeiro. A FAA passou a garantir imunidade para empresas que estivessem contribuindo para o governo, incluindo aquelas que violassem acordos de usuários e fossem contra a Lei de Comunicação de 1934 (ASSIS, 2020).

Para aumentar a capacidade de vigilância e coleta de informações dos EUA também foi desenvolvido o projeto Total Information Awareness (TIA). Inaugurado pela DARPA em 2002 com o objetivo de aumentar a capacidade do governo de identificar e classificar terroristas, o projeto encarou forte retaliação, sendo considerado uma afronta à privacidade de dados virtuais, e foi formalmente suspenso — entretanto, foi adotado por outras agências governamentais e posteriormente delegado para a iniciativa privada (ASSIS, 2020).

O Vale do Silício agora era responsável por continuar o extinto TIA, e inúmeras empresas da área de TI lucraram com contratos governamentais na área de inteligência, auxiliados pelas novas legislações criadas que favoreciam este tipo de relação. Empresas especializadas nesse mercado e grandes corporações, como o

Google e o Facebook, encontraram um nicho de mercado muito favorável ao seu crescimento (ASSIS, 2020).

> Nas palavras de Newton Lee (2014), as empresas privadas e a onipresença das redes sociais como Facebook, Google, Twitter e Youtube estão criando tecnologias e infraestruturas necessárias para colocar em prática, através de mecanismos civis, a proposta de projeto desenvolvido pela DARPA em 2002. Reconhecimento facial, rastreamento de localização, aplicativos sociais com rastreamento GPS e mineração de dados são alguns elementos chaves para a efetividade de um programa com as características do TIA. Havendo um claro entrelaçamento entre tecnologias militares e civis (LEE, 2014 *apud* ASSIS, 2020, p. 48).

Ao mesmo tempo em que o governo Bush desenvolvia legislações e tecnologias criadas para a vigilância digital, os Estados Unidos promovia uma política de liberdade de internet por todo o globo, a Global Internet Freedom Task Force (GIFT). Essa política tinha como objetivo promover o acesso a ideias e informações pela internet e impedir a censura virtual por parte de regimes autoritários, incluindo a promoção de um melhor acesso à internet e a disponibilidade de tecnologias de informação nos países em desenvolvimento — o que foi de grande interesse para o setor privado (ASSIS, 2020).

> O governo Bush estava pagando caro para desenvolver uma iniciativa diplomática de alto perfil capaz de moldar a internet e, ao disseminar seus tradicionais valores de proteção à democracia e aos direitos humanos, criar uma lógica totalmente fértil à expansão dos seus grandes monopólios de tecnologia, ao mesmo tempo em que internamente buscava flexibilizar a política que permitia que esses monopólios lhe concedessem acesso indiscriminado aos seus bancos de dados (GOLDSMITH, 2018 *apud* ASSIS, 2020, p. 55).

Mesmo com o início da administração de Barack Obama e com as denúncias realizadas em 2013 por Edward Snowden, as relações entre governo e o setor privado de tecnologia apenas se fortaleceram, muito em parte ao *Cybersecurity Act 2015*. A nova lei surgiu inicialmente como Cyber Intelligence Sharing and Protection Act (CISPA), foi renomeada como Cybersecurity Information Sharing Act (CISA) e, finalmente, foi sancionada pelo presidente em 2015 como *Cybersecurity Act*. Tal jurisdição beneficia a iniciativa privada ao garantir autonomia às empresas em termos de monitoramento de ameaças cibernéticas, o uso de medidas defensivas contra estas e o compartilhamento de informações dentro do setor e junto ao governo (ASSIS, 2020).

As revelações de Snowden, junto com o programa PRISM, mostraram ao mundo como a Agência de Segurança Nacional dos Estados Unidos (NSA) transformou grandes corporações de internet de abrangência global em um aparato

de coleta de inteligência, tudo com a ajuda dessa própria indústria. Mesmo depois que a comunidade internacional condenou o abuso de privacidade online nos EUA, mais notadamente a resolução da ONU condenando a vigilância ilegal e arbitrária, o Congresso dos EUA foi reticente em aprovar uma legislação abrangente para regulamentar a proteção federal de dados (ASSIS, 2020).

Em contrapartida, regimes autoritários e antidemocráticos, como China e Coreia do Norte, enxergam a expansão da internet e da liberdade de expressão como uma ameaça à soberania de suas nações. Estes países veem normas de censura e restrição de conteúdo online como uma medida de segurança estratégica contra mídias de comunicação online que poderiam ser usadas para espionagem ou ataques cibernéticos (ASSIS, 2020).

A China, particularmente, utiliza do mundo cibernético para obter controle absoluto sobre sua população. Mesmo que a constituição do país forneça a seus cidadãos liberdade de expressão e de imprensa em teoria, a opacidade das regulamentações da mídia chinesa permite que as autoridades reprimam qualquer oposição, alegando que elas expõem segredos de Estado e colocam a nação em risco (XU, 2014).

A mídia tradicional e os novos meios de comunicação têm sido rigorosamente controlados pelo governo chinês há décadas a fim de evitar a subversão potencial de sua autoridade. As táticas do regime muitas vezes envolvem controles rigorosos da mídia através de sistemas de monitoramento e firewalls, bem como o fechamento de publicações ou websites e a prisão de jornalistas dissidentes, blogueiros e ativistas. Além disso, especialistas afirmam que a censura da internet chinesa inclui métodos técnicos como a imposição de limites à banda larga, filtragem de palavras-chave, bem como o bloqueio indiscriminado de acesso a sites — e todos aqueles que o governo julgar como uma ameaça podem ser presos sem aviso prévio (XU, 2014).

> [...] Em 2009, o ativista de direitos humanos Liu Xiaobo foi condenado a onze anos de prisão por defender reformas democráticas e liberdade de expressão na Carta 08, que lhe valeu o Prêmio Nobel da Paz. Os censores bloquearam rapidamente as notícias do prêmio na China. Um ano depois, o jornalista Tan Zuoren foi condenado a cinco anos de prisão por chamar a atenção para a corrupção do governo e a má construção de prédios escolares que desabaram e mataram milhares de crianças durante o terremoto de 2008 na província de Sichuan. O governo chinês bloqueou todas as investigações sobre o assunto e os voluntários de Tan foram perseguidos e espancados. No início de 2014, o governo entregou uma sentença de prisão de quatro anos ao ativista de direitos humanos Xu Zhiyong, que, segundo observadores, foi o alvo devido à sua crescente presença nas plataformas de mídia social chinesas (XU, 2014).

Mais perturbador que isso é o futuro Sistema de Crédito Social (SCS); combinando vigilância em massa, tecnologias de reconhecimento facial e *Big Data*, o SCS é enquadrado como um conjunto de mecanismos que proporcionam recompensas ou punições como feedback aos atores, baseado não apenas na legalidade, mas também na moralidade de suas ações, abrangendo a conduta econômica, social e política (CREEMERS, 2018).

> Este objetivo maximalista, combinado com a proeza tecnológica em rápido crescimento da China, a ausência de fortes proteções constitucionais para os cidadãos individuais e a virada para um controle mais rígido do partido sob a administração Xi Jinping, levaram numerosos observadores a retratar o SCS como um pesadelo orwelliano, onde o Big Brother e Big Data conspiram para finalmente perceber os impulsos totalitários dos líderes autocráticos da China (CREEMERS, 2018, p. 2, tradução do autor).

Além de acompanhar os movimentos e ações dos cidadãos individuais, o sistema geraria uma pontuação numérica para cada pessoa. Tal sistema seria determinado por pontos de dados, incluindo compras on-line, postagens em redes sociais e o ciclo de amigos de um indivíduo. Assim, a pontuação teria um amplo impacto na vida das pessoas, afetando sua capacidade de conseguir empregos, empréstimos e hipotecas e seus relacionamentos com a família e amigos (CREEMERS, 2018).

O SCS, já utilizado em algumas regiões do país, é a ferramenta perfeita para coagir a população chinesa a seguir à risca as vontades do Partido Comunista da China (PCC). Qualquer cidadão que ousar falar ou se comportar de forma contrária às intenções do governo pode, automaticamente, ser rebaixado a um cidadão de segunda categoria, perdendo direito a benefícios como escolas particulares, universidades, viagens de trem e avião, além de sofrer constrangimento social e poder ser encarcerado (ISCHINA'S, 2021).

A China e os EUA são apenas dois exemplos de como o Estado pode utilizar do domínio cibernético como uma forma de vigilância em massa e controle social — pode-se entender que a ideia do ciberespaço como uma nova fonte de ameaças que podem vir a destruir e arruinar estruturas físicas e sociais, causando fatalidades inimagináveis foi exagerada justamente para tornar a população tão apreensiva e insegura, que ela passe a aceitar qualquer decisão tomada por governos, por mais invasivas que forem, apenas para sentir-se segura novamente (DUNLAP JUNIOR, 2014).

4.3 A AÇÃO DO ESTADO NO CIBERESPAÇO E SUA INFLUÊNCIA NO SISTEMA INTERNACIONAL

Foi possível observar, ao longo do capítulo quatro, que, longe de ser uma ameaça incontrolável da forma como muitos interpretam, o ciberespaço se assemelha mais a uma nova ferramenta de guerra e controle incentivada, financiada e desenvolvida pelas mãos do poder estatal, além de criada para cumprir as necessidades de governos nacionais — países desenvolvidos do Norte global, são os que mais se beneficiam de sua utilização estratégica.

Mesmo que um país como os EUA tenha se tornado inevitavelmente mais vulnerável ao conectar grande parte de sua infraestrutura com a internet e difundir a utilização da internet globalmente, ele tornou inúmeros aliados e inimigos, principalmente Estados em desenvolvimento, vulneráveis a invasões ou espionagem. Ameaças originadas não vêm de grupos extremistas religiosos ou de ativistas políticos, mas provavelmente de organizações nacionais de inteligência estrangeiras. Como uma análise histórica demonstra, a NSA representa uma ameaça cibernética muito maior do que o Estado Islâmico ou o *Anonymous*, especialmente considerando o caso do Brasil e a espionagem sobre as conversas privadas da ex-presidente Dilma Rousseff (KSHETRI, 2014).

Foi possível perceber, também, que escândalos como o caso da *Cambridge Analytica* são apenas o subproduto da sociedade hiperconectada, que o próprio governo norte-americano incentivou ao longo das últimas décadas, com o objetivo de obter rápido e fácil acesso a informações pessoais de bilhões de indivíduos internacionalmente. Na realidade, um dos primeiros e maiores clientes do SCL Group foram as forças armadas norte-americanas.

Então, apesar de que ataques cibernéticos e a guerra da informação possam causar turbulências na balança de poder inerente ao SI, estes novos fenômenos apenas tornarão o conflito mais desigual, pendendo a favor dos grandes Estados que já possuem a capacidade de utilizar do mundo virtual de forma estratégica e eficaz. Atores não estatais, usando apenas de armas cibernéticas, poderão perturbar a paz, mas nunca a ponto de romper a soberania de uma nação.

5 CONSIDERAÇÕES FINAIS

O desenvolvimento da Internet das Coisas e do *Big Data*, em conjunto com o paradigma teórico da interdependência complexa como parte do SI, dá a entender que as RI sofrerão uma revolução na qual cada pré-concepção teórica clássica torna-se obsoleta frente às mudanças de paradigma trazidas pelo mundo cibernético. Fronteiras físicas perderão seu valor em relação ao fluxo incontrolável de informações pelo mundo digital, atores não-estatais desafiarão a legitimidade de Estados e nenhum indivíduo estará longe do alcance do ciberespaço.

Realmente, o mundo virtual trouxe mudanças em termos de política, economia e segurança — assim como em termos do cotidiano da população comum que praticamente nenhum autor até a primeira metade do século XX foi capaz de prever. O aumento da globalização, aliado a desenvolvimentos em tecnologia imprescindíveis, trouxe consigo uma série de novos desafios para os quais a sociedade internacional ainda há de encontrar soluções e respostas. A criação e implementação de legislações internacionais que contribuam na regulação da utilização da internet entre fronteiras, e a criação de leis que regulam a coleta e o uso irrestrito de dados pessoais são exemplos de ações a serem tomadas pela comunidade internacional.

Entretanto, como observado ao longo deste trabalho, o ciberespaço não será o fim do SI, e a maneira hiperbólica sobre como são tratados os novos fenômenos inerentes ao mundo cibernético na mídia popular e por alguns acadêmicos, é responsável por criar uma ideia um pouco exagerada de que um ataque cibernético será o equivalente a um ataque nuclear. Criou-se uma noção generalizada de Estados sendo arrasados por ciberataques e exércitos sendo paralisados por hackers, o que ainda, por enquanto, está distante da realidade (VALERIANO, MANNESS, 2018).

Através de um olhar pragmático, é possível perceber que até mesmo os casos mais emblemáticos de ataques cibernéticos, como o *Stuxnet*, ou o caso da Estônia, provocaram danos insignificantes no longo prazo e não ocasionaram em nenhuma fatalidade. A grande maioria de ciberataques conhecidos até hoje serviram mais como uma oportunidade para grandes Estados, como Rússia e EUA, de flexionarem suas capacidades cibernéticas para o mundo do que para atingir algum objetivo militar (MUTI, TAJER, MACFAUL, 2014).

Como afirmado no quarto capítulo, mesmo que o custo de entrada para operar no mundo digital seja extremamente baixo, permitindo que qualquer grupo ou indivíduo utilize dele, o nível de coordenação e sofisticação necessários para se realizar um ataque ou invasão eficaz são muito altos. Grupos terroristas ou ativistas podem usar o ciberespaço como uma maneira de angariar fundos, atrair membros ou difundir suas ideias. Mas, sem a combinação de outros recursos estratégicos, somente através da internet, a atuação desses grupos é limitada (MESQUITA, 2019).

Esta pesquisa teve como objetivo verificar como os atores não-estatais e estatais utilizam de novas tecnologias no ciberespaço e sua influência no SI. Esse objetivo foi desenvolvido ponderando, entre outras questões, de que maneira essas novas tecnologias trazidas pelo domínio cibernético poderiam ser convertidas em armas de ataque; o que foi possível de se perceber é que o mundo virtual não se tornará uma arma por si só, mas sim uma ferramenta para auxiliar em operações político-militares (MUTI, TAJER, MACFAUL, 2014).

Grupos insurgentes não possuem a capacidade de utilizar do domínio cibernético em conjunto com um ataque cinético devido a complexidade e a alta necessidade de coordenação necessária para se realizar uma operação dessa natureza. Entretanto, como foi visto com a Operação Pomar e outros exemplos, exércitos nacionais podem coordenar ataques cibernéticos com ataques bélicos para debilitar forças inimigas (MUTI, TAJER, MACFAUL, 2014).

Contudo, o uso do ciberespaço como uma arma de guerra pode ainda não constituir uma ameaça para o SI, mas a sua utilização como uma ferramenta de manipulação em massa pode trazer grandes repercussões — nunca foi tão barato influenciar a opinião de milhões de pessoas simultaneamente. Com o *Big Data*, é possível descobrir cada detalhe da vida e personalidade de um indivíduo, e descobrir exatamente onde cutucá-lo para atrair sua atenção (ZWITTER, 2015).

Estados autoritários, como a China, usam do ciberespaço para vigiar cada movimento e pensamento de sua população. Não apenas existem milhões de câmeras instaladas com *softwares* de reconhecimento facial por todo o país, mas a internet é completamente monitorada e censurada. Os únicos sites que cidadãos chineses podem acessar são extremamente limitados e apenas demonstram aquilo que o governo aprova, manipulando a população em acreditar apenas naquilo que o PCC deseja.

Mais problemático para o SI, entretanto, é a utilização do ciberespaço como uma ferramenta de manipulação por grupos privados. Apesar de ser apenas um resultado de uma longa campanha política e de inteligência por parte dos Estados Unidos para poder monitorar o mundo inteiro, o capitalismo de vigilância e a guerra da informação agora fugiram do seu controle. A capacidade de empresas como o SCL Group de manipular votações em praticamente qualquer país, sem que a população sequer imagine estar sendo influenciada, representa um poder disruptivo para o qual ninguém ainda possui uma prevenção concreta (PRIVACIDADE, 2019).

Mesmo que alguns Estados tenham implementado leis para tentar limitar e controlar a quantidade de dados pessoais que empresas e organizações podem coletar de usuários na internet, como a General Data Protection Regulation (GDPR) na União Europeia ou a Lei Geral de Proteção de Dados (LGPD) no Brasil, seus esforços ainda são insuficientes para impedir a criação de campanhas de manipulação em massa.

Estas campanhas criadas por empresas publicitárias especializadas na utilização do *Big Data*, como já demonstrado no caso de Trinidad e Tobago, podem decidir o resultado de uma eleição ou decisão significativa de um Estado, como um referendo para uma nova constituição — o que inevitavelmente irá refletir no SI. Além disso, como foi possível perceber nas eleições estadunidenses de 2016 e 2020, e nas eleições brasileiras de 2018, este novo modelo de publicidade direcionada polariza a população cada vez mais, gerando instabilidade em cada nação (PRIVACIDADE, 2019).

Respondendo a pergunta-problema desta pesquisa: de que forma os atores estatais e não-estatais atuam no ciberespaço e influenciam o SI através dele: o mundo virtual entrega significativas vantagens para qualquer ator no cenário internacional que saiba usufruir corretamente de suas mecânicas. Contudo, contrário ao imaginário popular, na grande maioria dos casos os atores não utilizam de tecnologias digitais como uma arma de ataque, mas como uma ferramenta de influência.

Ambos atores, estatais e não-estatais, usam do ciberespaço para monitorar e manipular a opinião de pessoas desavisadas na internet, o que ao longo do tempo e em uma escala de milhões de indivíduos atingidos é suficiente para alterar a opinião pública sobre qualquer tópico. Tal fato, por sua vez, pode influenciar seriamente o SI ao passo em que sérias decisões políticas, tanto em âmbito nacional ou internacional,

podem ser tomadas baseadas em um voto popular manipulado pelo interesse de grupos privados — tal qual o caso do BREXIT.

Este trabalho foi escrito com a intenção de realizar uma exposição sobre tudo o que engloba o ciberespaço e como ele reflete em atores estatais e não-estatais e por consequência no SI. Ele é limitado, porém, em não explorar outros temas como a reflexão do ciberespaço em diferentes teorias de RI como o realismo ou marxismo. A partir disso, e considerando que ainda existe uma lacuna muito grande no campo das RI de trabalhos que explorem o mundo cibernético, esse projeto também existe como um incentivo a futuras pesquisas acadêmicas.

Tais discussões, presentes nesta pesquisa, são apenas pequenos retratos de uma realidade que está constantemente se expandindo e se desenvolvendo. O que foi visto até agora foram apenas os primeiros 20 anos do século XXI. Não há como prever que rumo o mundo digital tomará e tampouco quais serão as reações da comunidade internacional.

REFERÊNCIAS

AGOSTINI, Marcos Tocchetto. A CIBERNÉTICA SOB A ÓTICA DO FENÔMENO DA GUERRA E DA AGENDA DE SEGURANÇA. 2014. 92 f. TCC (Graduação) - Curso de Relações Internacionais, Universidade Federal de Santa Catarina, Florianópolis, 2014. Disponível em: epositorio.ufsc.br/bitstream/handle/123456789/124695/Monografia%20do%20M

ALEMANHA. MINISTÉRIO FEDERAL DO INTERIOR DA ALEMANHA. . **Cyber Security Strategy for Germany**. Berlim, 2021. Disponível em: https://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1. Acesso em: 21 abr. 2021.

APPS, Peter; FINKLE, Jim. **Suspected Russian spyware Turla targets Europe, United States**. 2014. Disponível em: https://www.reuters.com/article/us-russia-cyberespionage-insight-idUSBREA260YI20140307. Acesso em: 17 out. 2021.arcos%20Tocch etto%20Agostini.pdf? sequence=1&isAllowed=y. Acesso em: 18 abr. 2020.

ATAMAN, Muhittin. The Impact of Non-State Actors on World Politics: A Challenge to NationStates. Alternatives: Turkish Journal Of International Relations. Yalova, p. 42-66. Não é um mês valido! 2003. Disponível em: https://dergipark.org.tr/en/download/article-file/19401. Acesso em: 23 maio 2020.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **DOUTRINA MILITAR DE DEFESA CIBERNÉTICA**. Brasília: Ministério da Defesa, 2014. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf. Acesso em: 20 out. 2021.

BRONK, Chris. HACKS ON GAS: ENERGY, CYBER SECURITY, AND U.S. DEFENSE. In: DENI, John R. (ed.). **NEW REALITIES:**: energy security in the 2010s and implications for the u.s. military. Carlisle: Strategic Studies Institute, Us Army War College, 2015. p. 301-322. Disponível em: https://www.jstor.org/stable/resrep11987.18?seq=1#metadata_info_tab_contents. Acesso em: 17 out. 2021.

BUTCHER, Mike. **The CEO of Cambridge Analytica plans a book on its methods, and the US election**. 2017. Disponível em: https://techcrunch.com/2017/11/06/the-

ceo-of-cambridge-analytica-plans-a-book-on-its-methods-and-the-us-election/?guccounter=1. Acesso em: 23 out. 2021.

CADEMARTOR, L.H.u.; SANTOS, P.C.. A Interdependência Complexa e a Questão dos Direitos Humanos no Contexto das Relações Internacionais. **Revista Brasileira de Direito**, Florianópolis, v. 12, n. 2, p. 71-81, 18 dez. 2016. Complexo de Ensino Superior Meridional S.A.. http://dx.doi.org/10.18256/2238-0604/revistadedireito.v12n2p71-81. Disponível em: https://seer.imed.edu.br/index.php/revistadedireito/article/view/1584#:~:text=O%20presente%20artigo%20busca%20apresentar,economia%20nas%20rela%C3%A7%C3%B5es%20internacionais%20e. Acesso em: 18 abr. 2021.

CATIVO, Jorge. Como fazer a Metodologia em um Projeto? 2013. Disponível em: https://biblioteconomiadigital.com.br/2010/07/como-fazer-metodologia-em-um-projeto.html. Acesso em: 21 jun. 2020.

CREEMERS, Rogier. **China's Social Credit System: An Evolving Practice of Control**. 2018. 32 f. Dissertação (Mestrado) - Curso de Leiden Institute For Area Studies, Leiden University, Leiden, 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792. Acesso em: 14 out. 2021.

DEPARTAMENTO DE DEFESA DOS ESTADOS UNIDOS. **JP 1**: DOD Dictionary of Military and Associated Terms. Washington, D.C.: Departamento de Defesa dos Estados Unidos, 2021. Disponível em: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf. Acesso em: 14 jun. 2021.

DIANA, Juliana. Pesquisa descritiva, exploratória e explicativa. 2020. Disponível em: https://www.diferenca.com/pesquisa-descritiva-exploratoria-eexplicativa/#:~:text=A%20principal%20diferen%C3%A7a%20entre%20esses,para%20compree nder%20causas%20e%20efeitos. Acesso em: 21 jun. 2020.

DUNLAP JUNIOR, Charles J.. The Hyper-Personalization of War: cyber, big data, and the changing face of conflict. : Cyber, Big Data, and the Changing Face of Conflict. Georgetown Journal Of International Affairs, Washington D.c., p. 108-118, out. 2014. Disponível em: https://scholarship.law.duke.edu/faculty_scholarship/3381/. Acesso em: 18 abr. 2020.

ESTRE, Felipe Bernardo. Poder, interdependência e desigualdade.. In: 3° ENCONTRO NACIONAL ABRI 2011, 3., 2011, São Paulo. Proceedings

online... Associação Brasileira de Relações Internacionais, Instituto de Relações Internacionais - USP, Available from: <http://www.proceedings.scielo.br/scielo.php?script=sci_arttext&pid=MSC0000000122011000200007&lng=en&nrm=abn>. Acess on: 16 Nov. 2021.

FACCIONI FILHO, Mauro. **Internet das Coisas**. Palhoça: Unisulvirtual, 2016. 61 p. Disponível em: https://www.researchgate.net/publication/319881659_Internet_das_Coisas_Internet_of_Things. Acesso em: 20 jun. 2021.

FAOU, Matthieu. **FROM AGENT.BTZ TO COMRAT V4**: a ten-year journey. Bratislava: Enjoy Safer Technology (Eset), 2020. Disponível em: https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf. Acesso em: 17 out. 2021.

FREIRE, Antonio Rodrigo Candido. O NEOLIBERALISMO E A TEORIA DA INTERDEPENDÊNCIA COMPLEXA. 2012. Disponível em: https://www.jurisway.org.br/v2/dhall.asp?id_dh=7410. Acesso em: 21 jun. 2020.

GRAHAM-HARRISON, Emma; CADWALLADR, Carole; OSBORNE, Hilary. **Cambridge Analytica boasts of dirty tricks to swing elections**: bosses tell undercover reporters how honey traps, spies and fake news can be used to help clients. Bosses tell undercover reporters how honey traps, spies and fake news can be used to help clients. 2018. Disponível em: https://www.theguardian.com/uk-news/2018/mar/19/cambridge-analytica-execs-boast-dirty-tricks-honey-traps-elections. Acesso em: 20 out. 2021.

GUIMÓN, Pablo. “O ‘Brexit’ não teria acontecido sem a Cambridge Analytica”. 2018. Disponível em: https://brasil.elpais.com/brasil/2018/03/26/internacional/1522058765_703094.html. Acesso em: 21 jun. 2020.

ISCHINA'S Social Credit System Real? - I Found Out. Direção de Matthew Tye. Produção de Matthew Tye. S.I.: Laowhy86, 2021. (13 min.), P&B. Disponível em: https://www.youtube.com/watch?v=s22tMR4YoN0. Acesso em: 14 out. 2021.

KEOHANE, Robert Owen; NYE JUNIOR, Joseph Samuel. **Poder e Interdependência:**: a política mundial em transição. 5. ed. Oxford: Longman Classics, 1988. 368 p. Disponível em: https://www.skoob.com.br/poder-e-interdependencia-594086ed595307.html. Acesso em: 17 jun. 2021.

KSHETRI, Nir. Cybersecurity and International Relations: The U.S. Engagement with China and Russia. In: FLACSO-ISA JOINT INTERNATIONAL CONFERENCE, 1., 2014, Buenos Aires. Cybersecurity and International Relations: The U.S. Engagement with China and Russia. Buenos Aires: The University Of North Carolina, 2014. p. 1-38. Disponível em: http://web.isanet.org/Web/Conferences/FLACSOISA%20BuenosAires%202014/Archive/6f9b6b91-0f33-4956-89fc-f9a9cde89caf.pdf. Acesso em: 18 abr. 2020

MAIER, Friedrich. **A REVOLUÇÃO DA INFORMAÇÃO E O PODER CIBERNÉTICO: Um mapeamento conceitual na obra de Joseph S. Nye Jr**. 2016. 34 f. TCC (Graduação) - Curso de Relações Internacionais, Universidade Estadual Paulista "Júlio de Mesquita Filho" – Faculdade de Filosofia e Ciência de Marília (Ffc-Unesp), Marília, 2016. Disponível em: https://revistas.marilia.unesp.br/index.php/ric/article/view/6345. Acesso em: 14 fev. 2021.

MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco. The Fundamental Conceptual Trinity of Cyberspace. **Contexto Internacional**, Rio de Janeiro, v. 42, n. 1, p. 31-54, abr. 2020. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/s0102-8529.2019420100002. Disponível em: https://www.scielo.br/j/cint/a/WYHRGNsY5mpWzjCwsSfrTZv/?lang=en. Acesso em: 18 abr. 2021.

MESQUITA, Felipe Sousa. **Segurança Cibernética e a Política Internacional Contemporânea: novos desafios e oportunidades**. 2019. 38 f. Monografia (Especialização) - Curso de Curso de Especialização em Relações Internacionais, Universidade de Brasília, Brasília, 2020. Disponível em: https://bdm.unb.br/handle/10483/25026. Acesso em: 14 fev. 2021.

MINGST, Karen A.. **Princípios de Relações Internacionais**. 6. ed. Lexington: Gen Atlas, 2014.

MUTI, Alberto; TAJER, Katherine; MACFAUL, Larry. CYBERSPACE: AN ASSESSMENT OF CURRENT THREATS, REAL CONSEQUENCES AND POTENTIAL SOLUTIONS. **Remote Control**, Londres, p. 1-13, out. 2014. Disponível em: http://www.vertic.org/media/assets/Publications/CS1.pdf. Acesso em: 14 abr. 2021.

NERADKO, Kseniia. **A CYBER WESTPHALIA: CHALLENGING THE FIFTH DIMENSION**. 2018. 40 f. TCC (Graduação) - Curso de School Of Business And

Governance, Tallinn University Of Technology, Tallinn, 2018. Disponível em: https://digikogu.taltech.ee/et/Download/b4dc010b-fdcd-4a71-b99a-8275b935685b. Acesso em: 17 abr. 2021.

NYE JUNIOR, Joseph S.. **Cooperação e Conflito Nas Relações Internacionais**. Oxford: Gente, 2009. 73 p.

PRIVACIDADE Hackeada. Direção de Karim Amer Jehane Noujaim. Produção de Karim Amer Geralyn White Dreyfous Pedro Kos Judy Korin. Intérpretes: Carole Cadwalladr David Carroll Brittany Kaiser. Roteiro: Karim Amer Erin Barnett Pedro Kos. Sundance: The Othrs, 2019. (113 min.), son., color. Legendado. Disponível em: https://www.netflix.com/title/80117542. Acesso em: 21 out. 2021.

RANA, Waheeda. Theory of Complex Interdependence: A Comparative Analysis of Realist and Neoliberal Thoughts. **International Journal Of Business And Social Science**, Islamabad, v. 6, n. 2, p. 290-297, fev. 2015. Disponível em: https://www.ijbssnet.com/journals/Vol_6_No_2_February_2015/33.pdf. Acesso em: 14 abr. 2021.

REARDON, Robert; CHOUCRI, Nazli. The Role of Cyberspace in International Relations: A View of the Literature. In: 2012 ISA ANNUAL CONVENTION, 1., 2012, San Diego. **The Role of Cyberspace in International Relations.** San Diego: Department Of Political Science, Mit, 2012. p. 1-34. Disponível em: https://nchoucri.mit.edu/sites/default/files/documents/%5BReardon%2C%20Choucri%5D%202012%20The%20Role%20of%20Cyberspace%20in%20International%20Relations.pdf. Acesso em: 14 abr. 2021.

REEDER, Joe R.. Cybersecurity’s Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack. **The Cyber Defense Review (Cdr).** Washington, p. 15-39. jun. 2021. Disponível em: file:///D:/arquivos%20tcc/Cybersecuritys%20Pearl%20Harbor%20Moment%20(1).pdf. Acesso em: 18 out. 2021.

RIGAMONTE, Fernando Lira. **A SOBERANIA NA ERA CIBERNÉTICA**. 2017. 39 f. Monografia (Especialização) - Curso de Curso de Direito, Universidade Federal de Lavras, Lavras, 2017. Disponível em: http://repositorio.ufla.br/bitstream/1/30767/1/Fernando%20Lira%20-%20TCC.pdf. Acesso em: 14 fev. 2021.

SACCOL, Amarolinda Zanela. UM RETORNO AO BÁSICO: COMPREENDENDO OS PARADIGMAS DE PESQUISA E SUA APLICAÇÃO NA PESQUISA EM

ADMINISTRAÇÃO. Revista de Administração da Universidade Federal de Santa Maria, Santa Maria, v. 2, n. 2, p. 250-269, 30 jul. 2009. Disponível em: https://www.redalyc.org/pdf/2734/273420378007.pdf. Acesso em: 21 jun. 2020.

SANTAELLA, Lucia; GALA, Adelino; POLICARPO, Clayton; GAZONI, Ricardo. Desvelando a Internet das Coisas. **Geminis**, São Paulo, v. 1, n. 2, p. 19-32, 2013. Disponível em: https://www.revistageminis.ufscar.br/index.php/geminis/article/download/141/pdf/. Acesso em: 18 abr. 2021.

SANTOS, Bruno P.; SILVA, Lucas A. M.; CELES, Clayson S. F. S.; BORGES NETO, João B.; PERES, Bruna S.; VIEIRA, Marcos Augusto M.; VIEIRA, Luiz Filipe M.; GOUSSEVSKAIA, Olga N.; LOUREIRO, Antonio A. F.. Internet das Coisas: da Teoria à Prática. In: XXXIV SIMPOSIO BRASILEIRO DE REDES DE COMPUTADORES E SISTEMAS DISTRIBUđDOS (Bahia). **Livro de Minicursos SBRC 2016**. Salvador: Sociedade Brasileira de Computa¸c˜ao (Sbc), 2016. p. 1-329. Disponível em: https://bps90.github.io/assets/files/MinicursosSBRC2016.pdf. Acesso em: 20 jun. 2021.

SILVA, Alex Fiore da. **Big Data como Forma de Governança Racial**. 2018. 34 f. TCC (Graduação) - Curso de Direito, Universidade Presbiteriana Mackenzie, São Paulo, 2018.

TOMÉ, Luis. CIBERSEGURANÇA. 2013. 21 f. Tese (Doutorado) - Curso de Relações Internacionais, Universidade Autónoma de Lisboa, Lisboa, 2013. Disponível em: https://www.academia.edu/7610762/Departamento_de_Rela%C3%A7%C3%B5es_I nternacionai s. Acesso em: 18 abr. 2020.

VALERIANO, Brandon; MANESS, Ryan C.. International Relations Theory and Cyber Security. The Oxford Handbook Of International Political Theory, [s.l.], p. 258-272, 1 mar. 2018. Oxford University Press. http://dx.doi.org/10.1093/oxfordhb/9780198746928.013.19. Disponível em: https://www.researchgate.net/publication/326845990_International_relations_theory_ and_cyber_ security_Threats_conflicts_and_ethics_in_an_emergent_domain. Acesso em: 18 abr. 2020.

WILLETTS, Peter. Transnational Actors and International Organizations in Global Politics. The Globalisation Of World Politics, Oxford, v. 2, n. 1, p. 356-383, 2001. Disponível em:

http://biblioteca.cejamericas.org/bitstream/handle/2015/3651/TransnationalActors.pdf ?sequence =1&isAllowed=y. Acesso em: 23 maio 2020.

XU, Beina. **Media Censorship in China**. 2014. Disponível em: https://www.files.ethz.ch/isn/177388/media%20censorship%20in%20china.pdf. Acesso em: 14 out. 2021.

ZWITTER, Andrej. Big Data and International Relations. Ethics & International Affairs. Nova Iorque, p. 377-389. 11 dez. 2015. Disponível em: https://www.academia.edu/19657036/Big_Data_and_International_Relations. Acesso em: 18 abr. 2020.

ZWITTER, Andrej. Big Data ethics. Big Data & Society, [s.l.], v. 1, n. 2, p. 1-6, 10 jul. 2014. SAGE Publications. http://dx.doi.org/10.1177/2053951714559253. Disponível em: https://journals.sagepub.com/doi/10.1177/2053951714559253. Acesso em: 18 abr. 2020 \\]\]