

CIBER-RI: A PROJEÇÃO INTERNACIONAL DE PODER SOB A PERSPECTIVA DO SOFTWARE POWER

GALVÃO, Lorryne Rosa de Oliveira

RESUMO

Este trabalho tem por objetivo estabelecer ligações entre os processos históricos ocorridos durante o século XX e sua relevância ao desenvolvimento tecnológico, hoje considerado uma tendência notável e estudada no campo das Relações Internacionais, por auxiliar na compreensão do aperfeiçoamento social e econômico das nações, bem como na multiplicidade de ações que possibilitaram aos diversos atores do sistema internacional, desde os cidadãos, empresas, organizações até aos próprios Estados Soberanos. Serão abordados, respectivamente e em seções distintas, a fundamentação teórica utilizada no método de pesquisa, a saber as correntes realista e neoliberal, detentoras de conceitos primordiais que sustentam grande parte da estrutura teórica de RI; a esfera do Cyber Power apresentada por Nye Jr. e como esta nos ensina uma nova perspectiva do poder, existente no ciberespaço; e a instrumentalização do poder cibernético através do Software Power, termo desenvolvido por Gills Vilar Lopes e que representa alta relevância quanto a potencialidade de afetar o equilíbrio de poder interestatal e de gerar dominação por meio da manipulação de dados compartilhados através da rede de computadores conhecida mundialmente como internet.

PALAVRAS-CHAVE: Relações Internacionais, segurança, tecnologia, poder, ciberespaço, Software Power.

1 Introdução

As Relações Internacionais Cibernéticas constituem um campo recente que, desprovido de pesquisas aprofundadas, apresenta dificuldades em esclarecer o real impacto dos principais acontecimentos da era digital contemporânea, que tiveram reverberações a nível global e que modificaram substancialmente o modo como políticas de segurança são concebidas. Deste modo, a mobilização do arcabouço teórico tradicional de Relações Internacionais se faz necessário, na medida em que é imprescindível adequá-lo às relações de poder que acontecem no ciberespaço e que são refletidas nos fenômenos do sistema internacional (ERIKSSON & GIACOMELLO, 2006).

Destarte, a melhor maneira de assimilarmos o contexto no qual habitamos, e dentro do qual constituíram-se as relações internacionais cibernéticas, é através da digressão histórica, pois é sobre este recurso que se fundamenta a perspectiva de que o mundo do século XX já não é o mesmo do mundo hodierno. E embora seja esta uma afirmação óbvia, até o óbvio necessita ser dito quando, em claro equívoco, analisa-se anacronicamente a

contemporaneidade sob as lentes conceituais do passado. Com efeito, o final do século XX foi marcado por profundas modificações políticas e transformações nos processos de produção operantes até então, e a ampliação dos meios de comunicação em dimensões internacionais, que consequentemente contribuíram para o aumento no fluxo de informações, caracterizou um efeito inédito nas relações sociais, denominado globalização. Habilitou-se então a revolução nos termos operacionais das empresas, a criação de produtos capazes de reduzir o tempo e esforço em tarefas manuais ou que utilizavam a lógica e por isso necessitavam de métodos mais complexos. Um novo universo de possibilidades referente às relações de produção e as que ocorriam entre indivíduos foi descoberto, viabilizado através de aparatos tecnológicos inéditos, desenvolvidos tanto pela área de pesquisa e desenvolvimento computacional quanto por companhias de telecomunicação (GORENDER, 1997).

Mediante a abordagem hipotético-dedutiva dessa pesquisa, ou seja, de esforço analítico com o intuito de testar conceitos teóricos das RI que já estão estabelecidos, é elencado um novo vocábulo aos estudos sobre segurança internacional na era digital, que compreende o termo cunhado por Gills Vilar Lopes para denominar um novo instrumento de projeção de poder, o *Software Power*. O esforço de investigação aqui empreendido tem por finalidade esclarecer se o *Software Power* é, de fato, passível de ser aplicado no sistema internacional e se permite identificar os potenciais atores capazes de utilizá-lo, em última instância, como um meio para expandir a sua capacidade de dominação por influência, através do território virtual do ciberespaço (ERIKSSON & GIACOMELLO, 2006).

2 A Terceira Onda: evolução tecnocientífica do Século XX

Diante do desafio de analisar as contribuições dos estudos em Segurança Cibernética para as teorias de Relações Internacionais, considera-se necessário, a priori, realizar um exercício de digressão histórica, com o objetivo de esclarecer o modo como se deu o desenvolvimento tecnológico que sucedeu à criação do ciberespaço. Adotando os termos de Alvin Toffler, as revoluções industriais ocorridas em nossa história podem ser caracterizadas como “ondas” de desenvolvimento, que reverberaram não somente no aperfeiçoamento industrial, mas permitiram também a expansão do horizonte de interações sociais, que, por sua vez, geraram impactos políticos e econômicos em escala global, afetando diretamente a governabilidade dos Estados e seus atores domésticos (GORENDER, 1997; TOFFLER, 1999).

A Era de Ouro de meados do século XX impulsionou as bases de produção mundial localizadas nos países capitalistas desenvolvidos, enquanto que outras regiões mais pobres, como África e América Central, passavam por crises e impasses que limitavam o progresso industrial. As taxas de crescimento do comércio mundial dispararam ao ponto de se depararem com o que Hobsbawm enfatizou ser o “subproduto dessa extraordinária explosão, embora em retrospecto ele já parecesse ameaçador: a poluição e a deterioração ecológica” (2003, p.257). No entanto, mesmo a ameaça ao meio ambiente não pôde evitar que a ideologia progressista enfraquecesse: o avanço tecnológico adquirido a custos de degradação ambiental era convincente o bastante para perpetuar o comportamento negligente da produção capitalista de grande escala (HOBBSAWM, 2003; GORENDER, 1997).

Sob as circunstâncias do período, o modo de produção taylorista trouxe inovação aos métodos administrativos industriais, pautando-se no estudo dos processos produtivos para a dinamização do trabalho. Cada cargo foi instituído mediante tarefas específicas, que possuíam um tempo padrão de execução, de modo que movimentos desnecessários foram excluídos e o período de produção foi otimizado. Os funcionários passaram a ganhar salários diferenciados pelas suas aptidões e pelo rendimento de seu trabalho, e os indivíduos que exerciam as funções de gerência ficaram responsáveis, de acordo com Chiavenato (2004, p.57), pelo “estabelecimento dos métodos de trabalho e pela supervisão [...] durante a produção, enquanto o trabalhador fica somente com a execução do trabalho”. Sob esta ordem, foi instaurado que os cargos mais elevados na hierarquia corporativista ficariam incumbidos da função gerencial de “pensar” e demandar, enquanto que aos trabalhadores atribuiu-se apenas a execução das tarefas impostas. Foi o funcionário do chão de fábrica, juntamente com o auxílio de máquinas e equipamentos aprimorados para diversas funções, que proporcionou aos anos dourados o boom produtivo através da otimização no processo operacional das indústrias (HOBBSAWM, 2003; GORENDER, 1997; CHIAVENATO, 2004).

Levando em conta que o vigor da produção característica da Segunda Revolução Industrial depende, de modo crucial, do petróleo e seus derivados, sabe-se que estes são representantes de uma fonte de energia não-renovável, que necessita de instrumentos e máquinas de alto valor agregado para extração e refinamento. O valor dos barris de petróleo no ano de 1950 permaneceram, durante os vinte e três anos posteriores, abaixo da margem de dois dólares, e a tendência corrente de preços que barateou o petróleo só foi abalada com a primeira crise neste setor energético, em 1973. Embora os anos 1960 projetassem um cenário aparentemente promissor, Harvey contradiz essa percepção ao esclarecer que:

o ímpeto da expansão de pós-guerra se manteve no período 1969-1973 por uma política monetária extraordinariamente frouxa [...]. O mundo capitalista estava sendo afogado pelo excesso de fundos; e, com as poucas áreas produtivas reduzidas para investimento, esse excesso significava uma forte inflação (2008, p. 127)

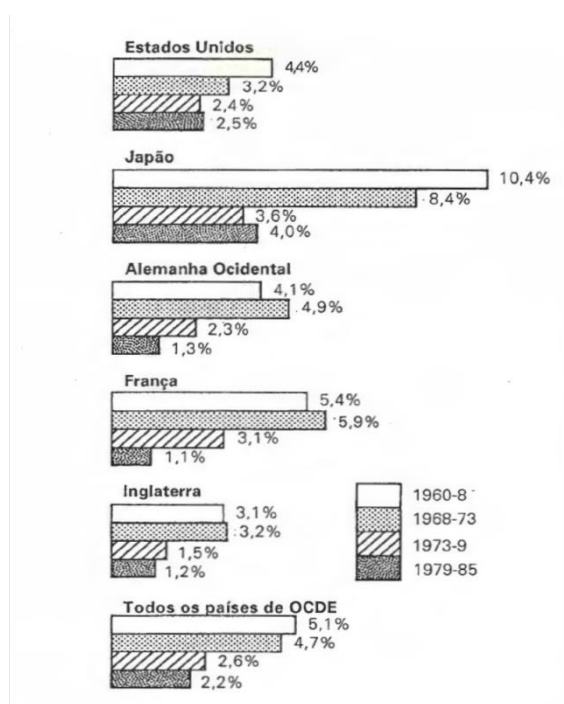
Ademais, era profundo o ambiente de tensão no Oriente Médio, influenciado sobretudo pelo revanchismo egípcio e sírio contra Israel, que deu lugar a um sentimento que não fora superado desde a Guerra dos Seis Dias, onde ambos os países perderam parcelas de território para os israelenses. Estes conflitos tanto se intensificaram que acabaram por atingir o status de conflito armado, e a Guerra do Yom Kippur constituiu-se em um dos conflitos regionais mais expoentes da época, juntamente com o movimento de efervescência das disputas interestatais entre Irã e Iraque. A decisão das companhias petrolíferas multinacionais em diminuir as taxas direcionadas aos países produtores de petróleo só fez agravar as contendas entre os membros da Organização dos Países Exportadores de Petróleo (OPEP) que, em contrapartida, revidaram aumentando exorbitantemente o valor dos barris, rompendo com o abastecimento internacional de óleo cru à diversas regiões vizinhas e do ocidente, retaliação essa que comprometeu todo o desenvolvimento econômico alcançado até o período. O choque causado por essa tomada de decisão alavancou, de forma inédita, este grupo de países de Terceiro mundo que, de outra forma, não seriam promovidos internacionalmente devido à sua pobreza e subdesenvolvimento. Todavia, apesar de reunirem grande riqueza em tão curto prazo, nas décadas seguintes países como a Arábia Saudita já haviam declinado ao endividamento (HOBSBAWM, 2003; HARVEY, 2008).

Compelida pela crise do petróleo, a divisão internacional do trabalho foi fadada a se adaptar ao transnacionalismo, ou seja, ao movimento de deslocamento das grandes empresas para além de suas fronteiras nacionais, que por conseguinte transferiu para o Terceiro Mundo o estoque de produção e o *know how* em processos industriais mais tecnologicamente aperfeiçoados, provenientes dos países do Primeiro Mundo. Consequentemente, pôde-se observar o avanço nos setores de comunicação e transporte, os meios mais relevantes pelos quais a globalização poderia ser difundida. A efervescência científica e tecnológica também fizeram com que a modernização dos países subdesenvolvidos se tornasse alvo para as críticas de grupos fundamentalistas e sua ideologia ortodoxa, como a reação do protestantismo contra tradicionalismo católico da América latina. Facilmente acessível, a informação estabeleceu uma conexão ainda mais forte entre as diferentes regiões do globo, desde as mais ricas e

desenvolvidas até as mais modestas e escassas em recursos. Os fluxos de migração construíram relações amplas e mais flexíveis entre as nações, tanto em termos laborais quanto sociais e culturais (HOBSBAWM, 2003; TOFFLER, 1999).

O crescimento econômico dos Estados capitalistas, que havia atingido altas taxas até a década de 1970, acabou por seguir níveis mais instáveis nos anos posteriores. A produção automobilística, naval, petroquímica e de eletrodomésticos compôs a força motriz deste processo, que se localizava predominantemente em grandes centros produtivos como nos Estados Unidos, Grã-Bretanha, Japão, Alemanha Ocidental e França, como está detalhado na Figura 1, a seguir:

Figura 1 – Transformação político-econômica do capitalismo



Fonte: HARVEY. 2008. Taxas anuais de crescimento econômico em países capitalistas avançados selecionados e da OCDE como um todo, segundo períodos de tempo selecionados, 1960-1985, 126. São Paulo.

Os demais países que, devido às guerras ocorridas décadas atrás, sofreram danos de difícil reparação, tiveram sua reestruturação facilitada pelos financiamentos provenientes dos Estados modernos do Primeiro Mundo, os quais utilizaram a operacionalidade das precursoras Tecnologias de Informação e Comunicação (TICs) para estruturar, flexibilizar e ampliar o acesso ao mercado financeiro (HARVEY, 2008; HOBSBAWM, 2003).

Desse modo, os grandes fluxos de capital enviados aos países periféricos estabeleceram um vínculo de dependência interestatal ainda mais complexo entre as potências

hegemônicas - avançadas em termos tecnocientíficos e de produção - e as economias periféricas - menos hábeis no aperfeiçoamento do processo produtivo e no processamento das matérias-primas. O papel estatal também foi crucial para efetivar a manutenção das políticas públicas, monetárias e fiscais a fim de sustentar o consumo em massa em relativa estabilidade, garantindo a maior parte dos empregos e disponibilizando auxílio em educação e saúde (HARVEY, 2008).

Os abalos na economia mundial que ocorreram nos últimos anos do século XX provocaram a oscilação necessária para que a Terceira Onda pudesse emergir. Uma vez que os Estados perceberam a necessidade de buscar outras fontes energéticas, de preferência renováveis e com custos menores, eles atentaram para os investimentos nas pesquisas em tecnologia. Foi no final do século XX que, como escreve Toffler, companhias como a Solarex e a Energy Conversion Devices tornaram-se pioneiras em pesquisa e desenvolvimento de painéis solares, constituídos por células fotovoltaicas, capazes de transformar luz solar em eletricidade e que hoje são utilizados em grande escala. Também nessa época, estudos feitos na Itália e Nova Zelândia buscaram desenvolver equipamentos que pudessem gerar energia através de fontes geotermiais e, no Japão, a obtenção de energia de ondas do mar tornou-se realidade (GORENDER, 1997; TOFFLER, 1999).

A partir do progresso tecnológico, decorreu o surgimento de disciplinas científicas como eletrônica quântica, biologia molecular, ecologia e a informática. A Revolução Científico-Tecnológica possibilitou a criação de máquinas hábeis em realizar cálculos e detectar padrões de programação que facilitassem o trabalho humano, além da invenção de aparelhos capazes de transmitir informações em velocidade, extensão e qualidade jamais alcançados em séculos anteriores. O ímpeto com o qual as Tecnologias de Informação e Comunicação (TICs) se desenvolveram decorre justamente dessa eficácia que elas demonstraram nos processos de receber informações e coordená-las de acordo com o fim para o qual foram projetadas. As TICs trouxeram dinamização aos sistemas corporativos; possibilitaram a disseminação de dados, independentemente do tempo e do espaço em que foram coletados; e modificaram profundamente o cenário internacional e doméstico dos Estados, revelando novas possibilidades de atuação para estes e os diversos atores que os constituem (GORENDER, 1997; TOFFLER, 1999).

O presente apanhado histórico sobre a revolução tecnológica viabilizará, a seguir, a análise pormenorizada dos desafios de adequação do arcabouço teórico de RI aos problemas de segurança enfrentados no século XXI, os quais constituem obstáculos não convencionais e por isso necessitam ser delineados, a fim de determinar qual a extensão dos seus efeitos na

elaboração de políticas de segurança e defesa, bem como sua influência no comportamento dos players internacionais. Deste modo, a categorização das perspectivas teóricas serão organizadas em dois grupos principais: Realismo e Neoliberalismo, cada qual possuindo diferentes níveis de interpretação e adaptação relativos ao estudo das Relações Internacionais Cibernéticas (ACAIO & GILLS LOPES, 2012).

3 Realismo e Neoliberalismo: embasamento conceitual para análise do Ciberespaço

Para que os objetivos do trabalho proposto sejam alcançados, faz-se necessário regressar a alguns conceitos e máximas que fundamentam as teorias em Relações Internacionais, como os que foram elaborados por autores clássicos da escola realista que, utilizando a racionalidade como ferramenta, buscavam superar o pensamento utópico com o intuito de construir considerações autênticas sobre o contexto internacional em que estavam inseridos. A partir das reflexões de Carr sobre os aspectos do Interesse Nacional, compreende-se que este tem origem e desenvolvimento proposital nos extratos sociais que mais detém poder e que mais possuem privilégios em uma nação, e que utiliza a ideia da harmonia de interesses como instrumento de legitimação para a prática de colocar interesses próprios como se fossem, de fato, nacionais. Entretanto, esta afirmativa não está errada, como elucida Carr:

A supremacia, dentro da comunidade, do grupo privilegiado pode ser, e frequentemente é, tão esmagadora que, de fato, em certo sentido seus interesses são o da comunidade, uma vez que seu bem-estar necessariamente traz consigo algumas medidas de bem-estar para outros membros da comunidade, e seu colapso poderia levar ao colapso da comunidade como um todo (CARR, 2001, p. 106)

É entendido, portanto, que quando a busca pelo interesse pessoal gera benefícios a outros indivíduos, os próprios atores desta busca são levados a acreditar que geram ganhos sociais, e tal relação de causalidade promove a manutenção deste comportamento específico. Aplicando a mesma lógica em uma esfera superior e em relação ao poder Estatal, compreende-se que o mesmo processo tende a ocorrer, mas em defesa de interesses relativamente cruciais como de preservação da paz e segurança internas, levando o Estado a necessariamente assumir o posicionamento condizente com a realização destes objetivos. Uma observação válida é que nem sempre os Estados vão agir de maneira pacífica ou em vias de cooperação pois, se for preciso ou vantajoso em termos de poder, os interesses destes atores vão levar a comportamentos hostis e até à contrapartida bélica a fim de que a paz seja preservada, o que representa um paradoxo inerente das relações internacionais (CARR, 2011;

MORGENTHAU, 2003).

O interesse definido em termos de poder representa um conceito que, como o próprio Morgenthau comenta, não pode ser delimitado permanentemente, mas sim ser compreendido como um interesse que, em sua essência, está em conformidade com intenções políticas. A incapacidade de demarcação conceitual, neste caso, advém das condições do contexto histórico ao qual se quer aplicar esta perspectiva, pois são muitas as variáveis socioculturais e econômicas que podem estar envolvidas neste âmbito de análise. O que é preciso ser feito é um esforço em utilizar o instrumento da lógica, para compreender o encadeamento das ações dos atores, cujos objetivos são alcançar resultados no âmbito político. Dessa forma, para que seja compreensível a relação entre os atores principais da teoria realista, os Estados, temos de explorar a dinâmica do equilíbrio de poder que existe no sistema internacional. Por definição, utilizaremos o termo cunhado por Morgenthau:

A aspiração de poder por parte de várias nações, em que cada uma tenta manter ou alternar o status quo, leva necessariamente a uma configuração que é chamada de equilíbrio de poder, bem como as políticas que se destinam a preservar esse equilíbrio. [...] O equilíbrio internacional de poder representa apenas uma manifestação particular de um princípio social de ordem geral, ao qual todas as sociedades compostas de um certo número de unidades autônomas devem a autonomia de suas partes componentes. [...]. Existem dois pressupostos na base de todas essas formas de equilíbrio: que os elementos a serem equilibrados são necessários para a sociedade ou têm direito de existir; e segundo: que, sem um estado de equilíbrio entre eles, um dos elementos ganhará ascendência sobre os demais, desrespeitará seus interesses e direitos e poderá finalmente destruí-los. (MORGENTHAU, 2003, p. 321)

É fundamental analisar o equilíbrio de poder no ambiente anárquico do sistema internacional porque, ao abranger os Estados como atores soberanos e de considerável autonomia, poderemos realizar comparações relativas ao sistema anárquico do espaço cibernético, verificar se é possível fazer uma analogia ao nível do equilíbrio de poder e estudar sua dinâmica nesta estrutura intangível, que proporciona novas formas de projeção de poder. A concepção de Morgenthau quanto a este equilíbrio vai além, ao abarcar níveis de subsistemas internos que se relacionam e afetam, diretamente e em última instância, a balança de poder internacional. As interações nestes subníveis ocorrem por meio da subalternidade a um conjunto de países dominantes de sistemas correlatos, que se encontram em um dos lados da balança; enquanto do outro, abrange um grupo diferente de países, com menos poder e influência. Sendo assim, com o fim da Guerra Fria entre os dois pólos de projeção de poder, a saber o norte-americano e o soviético, a dinâmica de estabilidade se transformou, e a balança

que antes se encontrava centralizada na Europa, terminou por se expandir mundialmente por meio da confirmação da hegemonia dos EUA (MORGENTHAU, 2003).

Em suma, o argumento oferecido pela afirmação da existência de um equilíbrio de poder foi legitimado porque tornou-se essencial para a manutenção da independência entre os Estados, mas isso não bastou para que as externalidades, ou os próprios países, deixassem de interferir nos assuntos e interesses uns dos outros. Por conseguinte, encontram-se lacunas na balança de poder à medida em que analisamos como ela é vulnerável e, consequentemente, incerta e inadequada à estrutura na qual o sistema internacional se fundamenta. Em contrapartida, ao aplicar a mesma lógica ao ciberespaço, observa-se que nele existem vulnerabilidades intimamente ligadas às novas capacidades de poder que, através dos instrumentos que a informática e tecnologia recentemente proporcionaram - como as TICs e os softwares - potencializa as interferências que os Estados podem exercer, propositalmente ou não, nas políticas externas ou de segurança dos demais países. Ao considerar este novo cenário de ação, a dinâmica da balança de poder é diretamente alterada, visto que a hegemonia no sistema internacional passou a ser mensurada, além da capacidade militar e potencialidade econômica, pela detenção de conhecimento e desenvolvimento tecnológico dos Estados. Isso realoca países como a China e Estônia para uma posição notável em termos de poder, o que caracteriza a mudança na interação entre os Estados no século XXI (MORGENTHAU, 2003; VALERIANO & MANNES, 2017).

Destarte, a definição de poder e seus aspectos são igualmente indispensáveis quando se versa sobre as questões de segurança e defesa internacionais. Para isso, as elucidações seguintes serão pautadas, essencialmente, no arcabouço teórico de Joseph Nye Jr. O poder pode se manifestar de inúmeras formas, embora as mais aparentes sejam as que envolvem controle e coerção, impostas a uma ordem sob a qual o risco de descumprimento é a repressão ou punição através da força e da violência, utilizadas nesse contexto como instrumentos, o que caracteriza um processo denominado por Nye como *Hard Power*. Nestes casos pode-se observar um dos principais pressupostos que definem o poder na prática: a influência direta no comportamento dos indivíduos. No entanto, o poder também possui a capacidade de se manifestar sob formas subjetivas e quase imperceptíveis, por meio de persuasão e motivação. Isso ocorre, por exemplo, com indivíduos que seguem rigorosamente dogmas religiosos, pois eles respeitam a autoridade moral que os estabeleceu. A esta categoria do poder dá-se o nome de *Soft Power* (NYE JR., 2004).

O poder também pode ser representado pela detenção de capacidades ou recursos que possam influenciar a obtenção de ganhos nacionais a níveis econômicos e sociais, mas esta

definição não é diretamente proporcional no sentido de que, quanto mais recursos e capacidades, mais ganhos. Isso ocorre porque as dimensões do poder são relativas e estão em constante mutação, e o modo como são utilizadas estas aptidões é o que vai determinar as vantagens e desvantagens, tanto a níveis nacionais quanto internacionais. Ou seja, não há garantias nas interações de poder entre os Estados, por isso são necessários estudos estratégicos intensos e hábil liderança governamental para traduzir recursos e capacidades em poder influente (NYE JR., 2004, 2011).

De maneira mais detalhada, a habilidade em influenciar as preferências dos outros é um dos trunfos do Soft Power, mas ele não se traduz somente a isso. Quando se obtém o apoio à líderes políticos através da atração pela autoridade moral, personalidade, cultura, valores políticos ou instituições, o controle e liderança em qualquer âmbito é facilitado, de tal forma que os objetivos políticos podem ser concretizados sem maiores preocupações ou custos, sejam eles monetários ou de prestígio. De acordo com Nye, o Soft Power está diretamente relacionado à persuasão e argumentação, que pela utilização de valores morais como justiça e dever, por exemplo, atraem os indivíduos e os motiva a cumprir o que fora estabelecido superficialmente como pedido ou necessidade, mas que é, em essência, uma ordem. Assim sendo, as fontes de Soft Power de um Estado provêm da cultura, de valores políticos domésticos e da forma como se relaciona com os atores externos. (NYE JR., 2004)

A cultura engloba todo o arcabouço de práticas e valores que dão sentido a uma sociedade. Um exemplo disso é o que conhecemos como o *American Way of Life*, que por meio do estilo de vida, as músicas, as marcas e a produção midiática norte-americana, influencia as nações de todo o globo. Observa-se que a cultura já não possui barreiras fronteiriças delimitadas, mas tornou-se um aspecto transnacional através das vias habilitadas pela globalização, onde o comércio e a internet representam os principais vetores dessa disseminação cultural. Os valores políticos domésticos e as relações exteriores dos países compreendem um tipo de Soft Power mais formal, porém também afetam as relações entre os Estados de forma significativa. Quando, por exemplo, uma política de segregação racial aconteceu nos EUA nos anos 1950, isso afetou diretamente seu Soft Power na África, pois gerou, nos africanos, aversão pelos valores sociais e políticos norte-americanos (NYE JR., 2004).

As teorias clássicas e contemporâneas aqui abordadas têm contribuições para a análise sistêmica do ciberespaço, porém também possuem suas limitações. Os axiomas realistas desconsideram os demais atores que interagem na estrutura internacional como, por exemplo, as organizações, empresas, instituições e os indivíduos. Dessa forma, visto que estes são

consideravelmente influentes no ambiente virtual, ao ignorá-los, o Realismo revela-se uma teoria insuficiente na investigação da multiplicidade de interações de poder, que ocorrem nas relações internacionais cibernéticas (ERIKSSON & GIACOMELLO, 2006).

Contudo, mesmo cientes da carência na abordagem dos demais atores, os teóricos realistas não julgam necessário examinar e reformular sua hipótese de modo a abarcar novos *players*, visto que, na sua percepção, a globalização e seus efeitos não destroem o princípio anárquico do sistema e, logo, os Estados continuam a exercer o papel mais relevante na era digital. Dessa maneira, costumam encarar as problemáticas que envolvem tecnologia e informação da mesma forma com que lidam com qualquer outro elemento que possa interferir nas políticas de segurança e na economia estatal. Exatamente por essa razão é que ciberespaço e seus recursos não são considerados pelos realistas como ameaças ou elementos com potencial de transformação radical da dinâmica estrutural do sistema, ao invés disso são vistos como fatores que perpetuam o princípio tradicional da segurança, de promover ataque ou defesa em prol da proteção à sobrevivência, soberania, interesse nacional e informação de que dispõem os Estados (ERIKSSON & GIACOMELLO, 2006).

Por ser mais abrangente, o liberalismo proporciona uma lente de análise mais voltada para a influência dos atores domésticos na conduta dos Estados no plano internacional; para a importância que possuem as instituições no momento de criação de regimes que constroem os *players*, e para os desafios que vão além das problemáticas provenientes da anarquia na arena internacional. Assim, mesmo que concordem com os realistas em relação à supremacia dos Estados, os liberais compreendem que grupos como os de movimentos sociais, de migrantes, corporações transnacionais, partidos políticos e até mesmo os grupos que atuam na esfera virtual, onde estão interconectados através das redes sociais, são relevantes na política internacional. Em termos de segurança, os governos tornam-se cada vez mais conscientes de suas capacidades limitadas em oferecer proteção necessária para a sociedade moderna, visto que eles mesmos enfrentam obstáculos na obtenção de *know how* e inovação em sistemas dos setores burocrático e militar. Deste modo, cabem aos grupos da sociedade, em contato com o ciberespaço, protegerem-se, com o que lhes é acessível, contra as ameaças de violação de dados e privacidade. Apesar de apresentarem desvantagens em matéria de proteção, os atores não-estatais crescem em quantidade e capacidade de projetar poder através da revolução da informação (ERIKSSON & GIACOMELLO, 2006; NYE JR., 2002).

Isto posto, a capacidade de influência do poder é relativa, ou seja, depende do contexto temporal no qual se encontram as políticas mundiais. Transformações no modo como a informação se expande sempre afetaram o poder, mas o domínio cibernético é um ambiente

inédito e extremamente volátil, concebido pelo próprio homem. As características do ciberespaço causam disparidades de poder entre os atores e, assim, representam um bom exemplo da distribuição desnivelada de poder que define a política global neste século, que ainda não proporciona a igualdade de recursos entre os atores. É por isso que, na sequência, a fim de compreendermos seu comportamento em outra dimensão, o poder será analisado dentro da esfera do ciberespaço (NYE, 2010).

4 Cyber Power e as Relações Internacionais

Dadas as anteriores elucidações acerca do Hard e Soft Power, conceitos teóricos notórios dentro do campo de estudos de Relações Internacionais, torna-se viável a discussão a seguir sobre a definição de *Cyber Power*, o qual apresenta-se essencial para o objetivo deste trabalho, que é o de analisar a ampliação de influência do poder pelas vias do ciberespaço, através das ferramentas de software. Esse elemento do poder, relacionado ao prefixo *cyber*, surge como a capacidade de controlar ou dominar os recursos disponíveis no ciberespaço tendo em vista um propósito, derivado não somente do Estado e seu interesse nacional, mas por outros atores, sejam eles civis, organizações ou empresas. A informação tornou-se, no século XXI, o instrumento do poder imaterial, o qual foi potencializado pela revolução tecnológica, pois ela proporcionou sua disseminação a nível global e habilitou a oportunidade inédita de também ampliar esse poder em áreas que antes eram de difícil acesso, seja em termos geográficos ou de resistência estatal ou social, e que agora podem ser analisadas e/ou influenciadas por meio da conexão com o ciberespaço (NYE, 2010).

Como vimos na primeira parte deste trabalho, a criação do primeiro espaço virtual de conexão entre máquinas, os computadores ARPANET, teve o propósito de facilitar o compartilhamento de informações e dados relativos aos do Departamento de Defesa norte-americano. A evolução tecnológica dos equipamentos eletrônicos e as pesquisas no campo da computação, que prosperaram depois do fim da Guerra Fria, ocasionaram também ameaças às máquinas e aos seus conteúdos compartilhados, através dos vírus e suas derivações, capazes de modificar, roubar, danificar e/ou destruir dados e informações armazenados em dispositivos eletrônicos. Como pode-se observar, o ciberespaço precisa possuir uma interface física para que seja acessado, o que lhe confere uma natureza híbrida singular. A sua porção física tende a seguir os padrões legislativos, econômicos e políticos, do respectivo espaço de soberania ao qual estão sob jurisdição. Por outro lado, sua porção virtual é autoexpansiva, de

modo que dificulta o controle jurídico das ações políticas exercidas neste espaço (NYE, 2010).

Para além da capacidade de expansão e alta flexibilidade do ciberespaço, o baixo custo de acesso ao ambiente virtual é um dos diferenciais mais atrativos para os atores que desejam exercer poder neste domínio. As forças terrestres, aéreas e navais necessariamente requerem grandes investimentos dos governos para que não apenas a segurança e defesa dos Estados sejam eficientes, mas para que também sejam capazes de alterar ou manter o equilíbrio na balança de poder internacional. Mesmo admitida a possibilidade de diversos players no domínio virtual, não significa que seus recursos de poder serão homogêneos, ou seja, ainda haverá demasiada desigualdade entre os atores. De modo mais aprofundado, podemos analisar o comportamento, trunfos e desvantagens dos agentes, através de sua categorização em três níveis: governamental, institucional e individual (NYE, 2010).

Os Estados e seus respectivos governos ainda são predominantes no campo de ação, tanto internacional quanto virtual, e isso acontece devido ao domínio de um espaço territorial, de uma infraestrutura interna e de maior aporte de recursos financeiros dos quais dispõem, que essencialmente são os tripés da soberania dos Estados no ciberespaço. De posse desses meios, os governos conseguem construir locais especificamente desenvolvidos para a educação e aperfeiçoamento tecnocientífico, que abastecem também o quadro de funcionários de setores estatais que envolvem a segurança nacional, como as agências de inteligência. Com sua maior capacidade de acesso ao mercado, os atores estatais detêm recursos suficientes para se projetar externamente e sustentar os orçamentos e a burocracia envolvidos nos esforços de defesa, além de terem como prerrogativa a legitimação do uso da força para garantir a coerção legal e física dos agentes que infringem ou contrariem suas leis e interesses. Contudo, apesar de dotados de tamanha capacidade de influência de poder, os Estados também possuem vulnerabilidades, dentre elas a dependência por sistemas complexos de gerência e armazenamento de dados que, quando acessados ilegalmente e com fins de espionagem, causam desvantagens em termos estratégicos pelo vazamento de informações, cujas consequências podem ameaçar a estabilidade política e a reputação dos países atingidos (NYE, 2010).

Temos as organizações internacionais e não-governamentais atuando no âmbito institucional dessa categorização, as quais têm a capacidade de mobilizar grandes orçamentos e recursos humanos, possibilitando-lhes operacionalizar grandes campanhas em prol de causas sociais através de recursos digitais, prática essa que é mais amplamente conhecida como ciberativismo. Contudo, assim como os Estados, as organizações também possuem

vulnerabilidades relacionadas ao seu prestígio, e podem ser acometidas pelo roubo de patentes, cometidos por usuários que agem ilegal e anonimamente (NYE, 2010).

Por conseguinte, os indivíduos que se encontram no último patamar de segmentação não podem ser menosprezados apenas por disporem de recursos financeiros inferiores aos dos grupos citados anteriormente. Devido às ínfimas barreiras de entrada ao ciberespaço, atores não Estatais também tem a capacidade de desempenhar funções relevantes na arena virtual, graças ao seu maior contingente numérico, e que por sua vez detém acesso quase ilimitado às informações e oportunidades viabilizadas pela internet. A nível particular, o agente não precisa necessariamente preocupar-se com a sua reputação, posto que lhe é proporcionada a vantagem de agir anonimamente. No entanto, o risco de ser descoberto permanece, e caso o agente seja pego, sua principal vulnerabilidade será a de sofrer a coerção legal por parte das organizações ou governos afetados (NYE, 2010).

É importante desmistificar a ideia de que o ciberespaço é inteiramente uma “terra sem lei” e necessariamente representa um bem público ou global, tal como são classificados os mares. No domínio virtual, também, há de se encontrar áreas privadas que estão sob controle soberano, observáveis através da análise dos processos de criação de padrões da rede, desenvolvidos pelos engenheiros responsáveis pela elaboração dos protocolos da World Wide Web, chamados de Internet Engineering Task Force (IETF). Essa equipe, por vezes, necessita das decisões de corporações privadas sobre seus produtos comerciais, as quais são balizadas pelas leis nacionais relativas à Direitos Autorais e de Propriedade Intelectual. A atuação governamental também abrange a responsabilidade pela alocação nacional da estrutura de comunicação, que foi negociada no acordo que instituiu a União Internacional de Telecomunicações, uma agência criada no âmbito das Nações Unidas em meados do século IX e que se dedica às questões que envolvam a coordenação global das TIC’s. Ainda que os governos se esforcem em gerenciar problemas de segurança cibernética conforme seus princípios nacionais legais, a capacidade de governança permanece falha por efeito da volatilidade do espaço virtual, o qual conturba a regulamentação jurídica devido aos seus alvos estarem em constante adaptação e deslocamento (NYE, 2010; ONU BRASIL, 2018).

Há maneiras de gerar *Hard Power* no ciberespaço quando, por exemplo, são provocadas interrupções ilegais nos sistemas e servidores de internet de um Estado ou companhia. Isso geralmente ocorre através de ataques realizados por “*botnets*”, redes de computadores interligadas por meio de um bot, uma espécie de malware que infecta milhares de computadores e os utiliza como “zumbis”, de modo a controlar suas atividades na internet sem que o próprio usuário da máquina perceba. Por serem redes extensas, os ataques de

botnets causam sobrecarga no sistema alvo, o que, por sua vez, produz instabilidade e inutilização temporárias. Os criminosos que aplicam esse tipo de ataque o fazem ou com o propósito de extorsão, sob a ameaça de contrapartidas mais ofensivas, ou para desarticular as capacidades do alvo, caso não tenham suas demandas atendidas. O conflito cibernético entre Rússia e Estônia em 2007 é um exemplo elucidativo dessa questão (NYE, 2010; THE GUARDIAN, 2007).

As conturbações entre os dois países tiveram início após a remoção da escultura Soldado de Bronze da capital da Estônia, Tallinn. Considerado um importante memorial de guerra da União Soviética, a intenção dos estonianos em mudar o monumento de localização causou revolta nos nacionalistas russos, a ponto de levá-los a empreender em uma ofensiva cibernética através de ataques Distribuídos de Negação de Serviço, ou os chamados DDDos. Essa categoria de ataques é, sobretudo, caracterizada pela interdição de sites ou sistemas devido à sobrecarga de acessos que recebem em um curto espaço de tempo, sendo estes acessos realizados pelos milhares de computadores zumbis interligados sob o controle de uma botnet. Na Estônia, foram alvos dos ataques os sites dos ministérios do governo, bancos, sistemas de empresas privadas e jornais, causando alarde até mesmo aos especialistas da OTAN, que foram mandados ao país para que investigassem o caso e auxiliassem no reforço da segurança cibernética estoniana (NYE, 2010; THE GUARDIAN, 2007).

Há também o espaço para a atuação Soft Power na internet, como é possível observar nos variados casos de ciberativismo que ocorrem na rede, prática exercida por grupos de indivíduos que possuem determinada motivação política, e que procuram atrair maior apoio social e promover mobilizações mais expressivas. A Primavera Árabe é um dos exemplos mais representativos do Soft Power do ciberativismo e este, no caso, foi potencializado após o falecimento de Mohamed Bouazizi, um comerciante tunisiano que ateou fogo em si mesmo em protesto aos abusos e injustiças feitos por agentes do governo, logo que policiais confiscaram sua banca, na qual vendia alimentos para o próprio sustento (NYE, 2010; ALJAZEERA, 2011).

A partir deste acontecimento, a internet foi utilizada de forma massiva pela população árabe, a fim de mostrar ao mundo a opressão que assolava a região e, ao mesmo tempo, levar maiores informações sobre a dimensão da crise pela qual passavam, visto que qualquer outro meio de comunicação como TVs e rádios estavam estritamente sob controle estatal. A reunião entre os países da Liga Árabe, em 2011, alertou aos governantes regionais que a rebelião tunisiana era uma ameaça iminente, e dentre os governos totalitaristas do Oriente Médio, como o de Ben Ali, na Tunísia, os movimentos revolucionários contra Muamar

Kadhafi, na Líbia, chegaram a atingir o nível de guerrilhas armadas, que lutaram contra as próprias tropas ditatoriais de Khadafi em vias de dismantelar seu governo. A reverberação do conflito assumiu tamanha gravidade que muitos revolucionários foram fatalmente eliminados até que Muamar fosse assassinado, e seu regime desintegrado (ARAB, 2011).

Como efeito do contexto caótico pelo qual passava o mundo árabe, pôde-se observar o redirecionamento e adaptação substancial dos governos para um posicionamento mais brando e com características democráticas, a fim de entrar em consonância com a democratização da Tunísia e facilitar as relações tanto políticas e econômicas regionais, mas ainda sim a instabilidade permaneceu, potencializada pelo uso das redes sociais na organização dos movimentos sociais. No Egito, por exemplo, a aparente sensação de que a transição para um regime democrático libertaria de vez os egípcios da tirania ditatorial ofuscou à população a real fragilidade política do Estado, que não se fortaleceu nem mesmo perante a resistência popular egípcia, simbolizada na manifestação na Praça de Tahrir em janeiro de 2011, motivada pela declaração de renúncia do ditador Hosni Mubarak. Após o curto período de um ano, um novo golpe militar foi imposto, que levou Abdel Fattah Al-Sisi a assumir novamente um poder ainda mais autoritário sobre a nação, limitando ao extremo a liberdade de expressão dos cidadãos (KANDIL, 2011; HOWARD & HUSSAIN, 2011).

4. 1 Software Power: O instrumento de projeção de poder no Ciberespaço

Com o advento mais expressivo da Terceira Revolução Industrial, a internet possibilitou a criação de novas cadeias inter-relacionais, inovando as interações econômicas, políticas, sociais e ampliando o tráfego de informações de maneira colossal, bem como o universo de atores que se movem no plano internacional desde a segunda metade do século XX. As fronteiras receberam uma nova roupagem, habilitando outra lente analítica do poder, visto que este ganhou capacidades inéditas, as quais ainda precisam ser estudadas devido sua multiplicidade. Esse é o motivo pelo qual carecem de aprofundamento teórico e analítico para a compreensão do seu alcance no comportamento dos atores e na estrutura do sistema internacional (NYE JR., 2004; LOPES, 2017).

As interações sociais sofreram consideráveis modificações nos últimos 60 anos, e junto com estas transformações houve a criação de uma dimensão virtual e aparentemente sem limitações espaciais, para a qual as relações sociais foram transpostas e multiplicadas. À essa dimensão se deu o nome de ciberespaço e, de acordo com Gill Villar-Lopes “configura-

se não apenas como um lócus social para a interação de indivíduos, mas também para a atuação estratégica de Estados. Ele se torna, nesse último viés, um espaço para, dentre outros, a projeção de poder” (2017, p. 4).

Tendo em vista a prerrogativa do Estado de promover a segurança e a defesa dos seus recursos e de sua nação, quer seja por meio da força ou da dissuasão em vias de garantir a realização do interesse nacional, deparamo-nos com o fato de que o ciberespaço e as ameaças à integridade estatal e a privacidade de informações, que se originaram no vácuo virtual, colocam os formuladores das estratégias de segurança nacionais em estado de alerta. Foi preciso criar um campo de estudos no qual pudessem ser investigados o poder e as relações cibernéticas, assim como os efeitos da interação entre eles que pudessem afetar a soberania dos Estados, e deste contexto surgem as pesquisas em Segurança Cibernética no campo das Relações Internacionais (LOPES, 2017)

A evolução industrial concretizada sob a forma das TIC's é um fenômeno relevante de modo que, a partir dele, pode-se esclarecer como estes instrumentos tangíveis e intangíveis como aparelhos eletrônicos e espaço virtual se relacionam e a nova forma de projeção de poder que acionaram, qualificada como Software Power, que nomeada por Villar-Lopes consiste em:

[...] capacidade político estratégica de que dispõem Estados para intervir na política internacional ou externa de outro Estado via utilização de software. [...]. Nesse sentido, quando um software causa danos a outro software ou hardware sem que haja, para isso, intenção, ou seja, ocorrência de mera falha ou desatualização, não está se falando de Software Power nem de Segurança Internacional, mas, sim, de Segurança da Informação aplicada à Computação. Software Power, portanto, enseja uma intenção (LOPES, 2017, p. 4)

Não obstante, a interface física que possibilita acesso ao ciberespaço, já mencionada como sendo os hardwares, é o que viabiliza a utilização dos programas aos quais nos referimos como softwares. Contudo, em termos de política internacional, os hardwares tendem a ficar em segundo plano, e isso acontece pelo fato de que as armas no âmbito cibernético são os próprios softwares programados com a finalidade de atacar outros sistemas e danificar dados e processos que são organizados e regidos por programação. Para que esta funcionalidade seja caracterizada como projeção de poder, ou Software Power de fato, é necessário sobretudo que um Estado utilize um software com a intenção de afetar a política externa de outro Estado, a sua política interna ou o próprio equilíbrio de poder do sistema internacional. Com a finalidade de demonstrar como o Software Power é posto em prática, o

Caso Stuxnet será apresentado e analisado a seguir (LOPES, 2017).

O Stuxnet é classificado como um malware do tipo worm, ou seja, um software malicioso que não necessita de um programa hospedeiro para se propagar, como ocorre com um vírus, mas que se auto-replica e é capaz de gerar falhas de sistema operacionais e programas, bem como eliminar arquivos e manipular as ações de uma máquina. A primeira aparição do Stuxnet foi em 2010, quando foi detectado em computadores iranianos por uma empresa de segurança da Bielorrússia, a VirusBlokAda. Sendo programado de forma sofisticada e com um processo de funcionamento extremamente complexo, o worm tinha por principal missão infectar os computadores que controlavam as centrífugas de refinamento de Urânio do Irã. Essas centrífugas funcionam de forma a separar a parte leve do Urânio da porção mais densa, que é a porcentagem do elemento mais relevante no desenvolvimento do conhecimento e tecnologia nucleares. O processo de separação do Urânio pode levar de meses a anos de duração, para que se possa atingir resultados satisfatórios. Os sistemas industriais utilizados nos reatores iranianos afetados, como o de Bushehr, eram fabricados pela Siemens, empresa de origem alemã e especialista na produção de softwares de automação. Tendo-se em consideração o *modus operandi* do sistema das centrífugas, os criadores do Stuxnet detectaram falhas através das quais poderiam se inserir e replicar seu próprio código em partes específicas e estratégicas do sistema, modificando os comandos do sistema de automação para comprometer o perfeito funcionamento das centrífugas, provocando variações de velocidade dos motores de rotação e colocando a perder todo o avanço obtido na separação das porções de Urânio (PCWORLD, 2010; LOPES, 2017).

Destarte, as consequências para o Programa Nuclear Iraniano foram consideráveis, e pela distinta expertise empregada na construção do Stuxnet, além da vultosa quantidade de recursos necessários para seu funcionamento, que dificilmente poderiam ser custeados por grupos que não tivessem um descomunal aporte financeiro, é fortemente considerado que tenha sido projetado e financiado por algum Estado que tinha o progresso no setor nuclear do Irã como ameaça ao equilíbrio de poder na região. Logo, o que se pode compreender deste caso é que o Stuxnet foi criado por um Estado, com a intenção política de sabotar o avanço do Programa Nuclear de outro Estado, contudo sem eliminá-lo permanentemente. Assim sendo, é possível ver materializado o conceito de Software Power, sobre o qual se procurou versar neste trabalho (PCWORLD, 2010; NEXO, 2010; LOPES, 2017).

Se faz necessário também esclarecer a diferença entre o conceito de Software Power e Software Warfare, visto que em âmbito técnico ambos possuem semelhanças processuais, mas quando se inclui a perspectiva de finalidade de cada um, compreende-se que dispõem de

objetivos distintos. Como propõe Bellamy, o Software Warfare é o combate entre softwares desenvolvidos por forças militares de Defesa, que pretendem comprometer a capacidade operacional e tática do inimigo no terreno de combate físico, manipulando os códigos que coordenam as redes de computadores militares do adversário, bem como seus respectivos comandos e informações. O esclarecimento deste conceito leva a inferir que a guerra entre softwares possui finalidade limitada, e que se encontra dentro da esfera de instrumentos à disposição do Software Power, uma modalidade de projeção de poder que é envolvida pelo âmbito do Cyber Power, cuja aplicabilidade só pode existir dentro do ciberespaço (BELLAMY, 2001; LOPES, 2017)

É conhecido que a informação é mais um dos recursos empregados para manipulação do equilíbrio de poder, tanto no mundo real quanto no virtual. O Information Warfare, princípio também desenvolvido por Bellamy, relaciona-se à manipulação de informação que tem por intuito confundir a capacidade de julgamento do adversário e, assim, influenciar suas ações pela incapacidade de distinguir o fato verdadeiro do falso. Há diversas possibilidades de executar a Information Warfare, mas aqui a investigação basear-se-á no uso de softwares projetados especificamente para colher, armazenar e analisar quantidades descomunais de dados - que são os grandes conjuntos de informações chamados de Big Data - que possibilitam a descoberta de padrões de associação de dados e as tendências seguidas por determinados fluxos de informação. Todo este trabalho de mineração de dados é feito por programas sob a intenção de detectar vantagens competitivas nos setores em que são aplicados (BELLAMY, 2001; LOPES, 2017; NEXO, 2017).

Como exemplo de ator nesta prática está a Cambridge Analytica (CA), empresa britânica criada em 2013 e que tem por intuito utilizar a análise de Big Data para potencializar campanhas políticas. O método utilizado pela CA se fundamenta essencialmente no estudo de comportamento de milhares de indivíduos, feito por um software que utiliza como matéria-prima os dados que empresa tem acesso, categorizando-os em cinco parâmetros de personalidade, sendo eles: A) Openness: propensão à maior receptividade de experiências inéditas; B) Conscientiousness: grande estima pela capacidade de organização; C) Extroversion: comportamento pessoal que tende a taxas de relacionamento social maiores e que preserva uma perspectiva otimista de fatos e pessoas; D) Agreeableness: caracterizado pela aguçada sensibilidade de percepção de variados temas e inclinação à cooperação; e E) Neuroticism: aspecto comportamental relativo instabilidade emocional de um indivíduo. Juntos, estes aspectos criam o modelo Ocean de análise, que auxilia no aperfeiçoamento e direcionamento inteligente de propagandas de maneira seletiva e exclusiva, mediante os dados

disponibilizados pelos indivíduos através das redes sociais. O modo como a CA utilizou grande quantidade de dados pessoais e sem o devido consentimento dos cidadãos se tornou um assunto polêmico de dimensões internacionais, haja vista as acusações de manipulação da informação e opinião pública por parte da empresa, que afetou as tomadas de decisão em relação ao Brexit e também a eleição presidencial norte-americana em 2016, através da qual Donald Trump elegeu-se como presidente dos Estados Unidos mediante os serviços prestados pela Cambridge Analytica (BELLAMY, 2001; NEXO, 2017).

O controle da informação com a finalidade de empreender em esforços de guerra é denominado por Arquilla e Ronfeldt como *Cyber War*, que é um conceito essencialmente caracterizado pelo desenvolvimento ou aplicação de tecnologia na utilização das estratégias militares de conflito, visando transformar o conhecimento em capacidade, o que consequentemente possui implicações para a própria doutrina militar devido à necessidade de reorganização das rotinas administrativas e operações de inteligência. O ciberespaço certamente transformou-se em um novo âmbito para se fazer a guerra em nível operacional, que pode ser tão hostil quanto a guerra convencional em termos de dano às capacidades do alvo, que do mesmo modo podem afetar a infraestrutura do Estado atacado e causar transtorno aos civis, como efeito colateral das ofensivas cibernéticas feitas em prol de provocar danos aos sistemas públicos. De todo modo, há de se compreender que o ciberespaço é livre de vínculos morais, e isso muito o potencializa como instrumento de poder, o que gera implicações políticas que nem mesmo são totalmente conhecidas devido à sua volatilidade funcional, trazendo para as relações entre os Estados um novo elemento que pode ser, ao mesmo tempo, benigno ou ameaçador (CANABARRO & BORNE, 2015).

6 CONSIDERAÇÕES FINAIS

Os estudos sobre as Relações Internacionais Cibernéticas (CiberRI) são recentes, mas suas descobertas muito auxiliaram na análise da contemporaneidade conceitual das teorias de Relações Internacionais. Sendo assim, o presente trabalho almejou esclarecer em que medida o arcabouço teórico das RI contribui, ou não, para a compreensão da nova dinâmica atual de relações de poder cibernéticas, assim como para a reflexão de que se o conceito de Software Power é passível de ser aplicado como novo instrumento de projeção de poder.

Deste modo, ao contrapor o arcabouço teórico *mainstream* das Relações Internacionais com o presente cenário internacional, observa-se as limitações da utilidade dos conceitos

tradicionais e, ao mesmo tempo, a necessidade de se reformular as perspectivas hipotéticas sobre a aplicação destes, que não compreendem elementos atuais da realidade da segurança Internacional, por estarem desatualizados. Ainda que reconhecidos como clássicos dentro do campo de estudos das Relações Internacionais, e serem fatores estruturais para a construção de hipóteses sobre as pesquisas da área de CiberRI, estes princípios carecem de atualizações de definição, devido principalmente às transformações tecnológicas e sociais presentes no contexto histórico hodierno. Ao constatar o problema de adequação conceitual das Relações Internacionais relativas às questões de Segurança e Defesa Nacional e Internacional, afetadas pelo ciberespaço e sua inerente anarquia, buscou-se chegar às conclusões que possibilitem sugestões de adequação, assim como modelos de aplicação derivados dos reajustes feitos das concepções tradicionais do campo.

O conceito de Software Power foi testado e, por fim, considerado como um termo híbrido de aplicabilidade eficiente, fruto da junção entre a teoria internacionalista neoliberal de Nye Jr. e as comprovações factuais de desafios às políticas de segurança do século XXI, que já não podem mais serem observadas somente sob as lentes realistas sem que sejam ignoradas diversas variáveis relativas à natureza e quantidade dos atores, além de suas capacidades. Estes fatores tornam o Realismo uma teoria limitada e, por conseguinte, em plena era de informação e alta tecnologia, insuficiente na análise de projeção de poder no sistema internacional.

7 Referências

ACÁCIO, Igor Daniel P; SOUZA, Gills. **Segurança internacional no século XXI: o que as teorias de Relações Internacionais têm a falar sobre o ciberespaço?**. In: Encontro Anual da ANPOCS, 36., 2012, Águas de Lindóia. Política Internacional – GT28. São Paulo: Anpocs, 2012. p. 1 - 24. Disponível em: <<https://anpocs.com/index.php/encontros/papers/36-encontro-anual-da-anpocs/gt-2/gt28-2/8169-seguranca-internacional-no-seculo-xxi-o-que-as-teorias-de-relacoes-internacionais-tem-a-falar-sobre-o-ciberespaco>>. Acesso em: 11 out. 2018.

ALJAZEERA. **Arab leaders warned of ‘revolution’**: Arab League chief warns regional leaders that recent political upheaval is linked to deteriorating economic conditions. Al Jazeera, [S.l.], 19 jan. 2011. Disponível em:

<<https://www.aljazeera.com/news/middleeast/2011/01/2011119165427303423.html>>. Acesso em: 25 nov. 2018.

ARCON. **Desvendando uma Botnet**. 2017. Disponível em: <<https://www.arcon.com.br/blog/desvendando-uma-botnet>>. Acesso em: 07 out. 2018.

BULL, Hedley. **A Sociedade Anárquica**. 2002. Disponível em: <http://funag.gov.br/loja/download/158-Sociedade_Anarquica_A.pdf>. Acesso em: 10 maio 2018.

CANONGIA, Claudia; MANDARINO JUNIOR, Raphael. **Segurança cibernética: o desafio da nova Sociedade da Informação**. 2009. Disponível em: <http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/349/342> Acesso em: 05 de maio 2018.

CHIAVENATO, Idalberto. **Introdução à Teoria Geral da Administração**. 7. ed. Rio de Janeiro: Elsevier, 2004.

CLARKE, Richard A; KNAKE, Robert K. **Cyber War: the next threat to national security and what to do about it**. New York: HarperCollins, 2010.

CLAUSEWITZ, Carl von. **Da guerra**. São Paulo: Tahyu, 2005. GORENDER, Jacob. (1997). Globalização, tecnologia e relações de trabalho. *Estudos Avançados*, 11(29), 311-361. <<https://dx.doi.org/10.1590/S0103-40141997000100017>> Acesso em 26 de maio de 2018.

ERIKSSON, Johan; GIACOMELLO, Giampiero. **The Information Revolution, Security, and International Relations: (IR)relevant Theory?**. New York: Jstor, Vol. 27, No. 3. 2006.

G1. **Morre jovem que ateou fogo no próprio corpo na Tunísia**. 2011. Disponível em: <<http://g1.globo.com/mundo/noticia/2011/01/morre-jovem-que-ateou-fogo-no-proprio-corpo-na-tunisia.html>>. Acesso em: 01 set. 2018.

G1. **Saiba como age o vírus que invadiu usinas nucleares no Irã e na Índia**. 2010. Disponível em: <<http://g1.globo.com/tecnologia/noticia/2010/10/saiba-como-age-o-virus-que-invadiu-usinas-nucleares-no-ira-e-na-india.html>>. Acesso em: 07 out. 2018.

GORENDER, Jacob. **Globalização, tecnologia e relações de trabalho**. 1997. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40141997000100017>. Acesso em: 04 set. 2018.

HARVEY, David. **Condição Pós-Moderna**. 17. ed. São Paulo: Edições Loyola, 2008.

HOBBSBAWM, Eric. **A era dos extremos**. O breve século XX (1914-1991). São Paulo: Companhia das Letras, 2003.

HOWARD, P. N.; HUSSAIN, M.M. **The Role of Digital Media**. *Journal of Democracy*, [S.l.], v. 22, n. 3, p. 35-48, 2011.

KANDIL, H. **A revolta no Egito**. *Novos Estudos*, [S.l.], n. 91, pp. 155-193, 2011. Trad. Alexandre Morales. Disponível em <<http://dx.doi.org/10.1590/S0101-33002011000300009>> Acesso em: 21 nov. 2018

LOPES, Gills Vilar. **Relações internacionais cibernéticas (CiberRI): uma defesa acadêmica a partir dos estudos de segurança internacional**. 2016. 165 f. Tese (Doutorado) - Curso de Pós graduação em Ciência Política, Departamento de Ciência Política, Universidade Federal de Pernambuco, Pernambuco, 2016. Disponível em: <https://www.academia.edu/31120775/_TESE_DE_DOUTORADO_Rela%C3%A7%C3%B5es_Internacionais_Cibern%C3%A9ticas_CiberRI_uma_defesa_acad%C3%AAmica_a_partir_dos_Estudos_de_Seguran%C3%A7a_Internacional?auto=download> Acesso em: 20 de maio de 2018.

LOPES, Gills Vilar. **Relações Internacionais Cibernéticas (CiberRI): O Impacto dos Estudos Estratégicos sobre o Ciberespaço nas Relações Internacionais**. In: CONGRESSO LATINO AMERICANO DE CIÊNCIA POLÍTICA, 9., 2017, Montevideu. Congresso. Asociación Latinoamericana de Ciencia Política, 2017. p. 2 - 16. Disponível em: <<http://www.congresoalacip2017.org/archivo/downloadpublic2?q=YToyOntzOjY6InBhcmFtcyczozNToiYToxOntzOjEwOiJJRF9BUlFVSzVZPIjtzOjQ6IjMyMzAiO30iO3M67MT0iaCI7czozMjpmYmNkMDViYjk2NTFiNWRjMzI2OTRiMmUwZTVlNzciO30=&>> Acesso em: 20 de maio de 2018.

MATTHEWS, Ron; TREDDENICK, John. **Managing the Revolution in Military Affairs**. London: Palgrave, 2001. 294 p.

MORGENTHAU, H.. **A Política entre as Nações**. 2003. Disponível em: <http://funag.gov.br/loja/download/0179_politica_entre_as_nacoes.pdf>. Acesso em: 05 maio 2018.

MUNDO EDUCAÇÃO. **Primavera Árabe**. 2018. Disponível em: <<https://mundoeducacao.bol.uol.com.br/geografia/primavera-Arabe.htm>>. Acesso em: 01 set. 2018.

MUNDO EDUCAÇÃO. **Terceira Revolução Industrial**. 2018. Disponível em: <<https://mundoeducacao.bol.uol.com.br/geografia/terceira-revolucao-industrial.htm>>. Acesso em: 26 de maio de 2018.

NYE JR, Joseph S. **Soft power: the means to success in world politics**. Nova York: PublicAffairs, 2004.

NYE JR, Joseph S. **Cyber Power**. Cambridge: Harvard Kennedy School, 2010. 30 p.

NYE JR, Joseph S. **The Paradox of American Power: Why the World's Only Superpower Can't Go It Alone**, 2002. Oxford: Oxford University Press.

NYE JR, Joseph S. **The future of Power**. 1. ed. New York: PublicAffairs, 2011.

OFICINA DA NET. **Diferença entre: vírus, spam, spyware, worm, phishing, botnet, rootkit**. 2014. Disponível em: <<https://www.oficinadanet.com.br/post/12991-diferenca-entre-virus-spam-spyware-worm-phishing-botnet-rootkit>>. Acesso em: 07 out. 2018.

ONU. **UIT: União Internacional de Telecomunicações**. 2008. Disponível em: <<https://nacoesunidas.org/agencia/uit/>>. Acesso em: 12 nov. 2018

PCWORLD. **Was Stuxnet Built to Attack Iran's Nuclear Program?** 2010. Disponível em: <https://www.pcworld.com/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html>. Acesso em: 10 out. 2018.

SAS. Big Data: **O que é e qual sua importância?**. 2018. Disponível em: <https://www.sas.com/pt_br/insights/big-data/what-is-big-data.html>. Acesso em: 10 out. 2018.

THE GUARDIAN. **Iran 'detains western spies' after cyber attack on nuclear plant.** 2010. Disponível em: <<https://www.theguardian.com/world/2010/oct/02/iran-western-spies-cyber-attack>>. Acesso em: 07 out. 2018.

THE GUARDIAN. **Iran accuses Siemens of helping launch Stuxnet cyber-attack.** 2011. Disponível em: <<https://www.theguardian.com/world/2011/apr/17/iran-siemens-stuxnet-cyber-attack>>. Acesso em: 07 out. 2018

THE GUARDIAN. **Russia accused of unleashing cyberwar to disable Estonia.** 2007. Disponível em: <<https://www.theguardian.com/world/2007/may/17/topstories3.russia>>. Acesso em: 12 nov. 2018.

UNDERLINUX. **Cyberwarfare: entendendo o vírus Stuxnet e a nova guerra.** 2010. Disponível em: <<https://under-linux.org/entry.php?b=2274>>. Acesso em: 10 out. 2018.

VIRUSBLOKADA. **Vba32 Anti-virus.** 2018. Disponível em: <<http://anti-virus.by/en/index.shtml>>. Acesso em: 10 out. 2018.

VIZENTINI, Paulo Fagundes. **Os trinta anos da Guerra do Yom Kippur e do choque petrolífero.** 2003. Disponível em: <http://educaterra.terra.com.br/vizentini/artigos/artigo_133.htm>. Acesso em: 20 out. 2018.

WALTZ, Kenneth N. **Teoria das Relações Internacionais.** Lisboa: Gradiva, 2002.