UNIVERSIDADE CÂNDIDO MENDES
INSTITUTO UNIVERSITÁRIO DE PESQUISAS DO RIO DE JANEIRO
DEPARTAMENTO DE RELAÇÕES INTERNACIONAIS
Graduação em Relações Internacionais

Paulo Cesar Gomes dos Santos Júnior

O Uso do Ciberespaço para a Obtenção de Poder no Cenário Internacional durante o Início do Século XXI

Rio de Janeiro
2016

Paulo Cesar Gomes dos Santos Júnior

O Uso do Ciberespaço para a Obtenção de Poder no Cenário Internacional durante o Início do Século XXI

Monografia apresentada como pré-requisito para a conclusão do Curso de Relações Internacionais do Departamento de Relações Internacionais do Instituto Universitário de Pesquisas do Rio de Janeiro.

Orientador: Prof. Dr. Lier Pires Ferreira

Rio de Janeiro

2016

Paulo Cesar Gomes dos Santos Júnior

O Uso do Ciberespaço para a Obtenção de Poder no Cenário Internacional durante o Início do Século XXI

Monografia apresentada como pré-requisito para a conclusão do Curso de Relações Internacionais do Departamento de Relações Internacionais do Instituto Universitário de Pesquisas do Rio de Janeiro.

_____

Prof. Dr. Lier Pires Ferreira
Orientador/IUPERJ

_____

(leitor crítico)

Dedicado a todas as pessoas que anseiam por um mundo melhor e acreditam no potencial humano de superar os profundos abismos da guerra construindo pontes para a paz.

Nada mais inteligente do que o silêncio
da percepção profunda das coisas
Nada mais tolo do que o ruído estridente
da superficialidade mecânica
do desejo vazio e imediatista das coisas

Antônio Weissmann em "Canções do Novo Mundo"

O Uso do Ciberespaço para a Obtenção de Poder no Cenário Internacional durante o Início do Século XXI

RESUMO

O ciberespaço tem se consolidado como uma ferramenta indispensável para o funcionamento do mundo atual, seja pela cibercultura, resultado da interação espontânea entre as pessoas dentro da 'Era da Informação', seja pela presença cada vez mais pervasiva de meios eletrônicos de comunicação e processamento de dados em todos os níveis organizacionais da sociedade. Entretanto, à medida que o uso do ciberespaço se torna cada vez mais intenso, as grandes facilidades e possibilidades que ele oferece representam também novos desafios em termos de governança e segurança. As intervenções militares no ciberespaço, quase sempre realizadas em segredo ao mesmo tempo em que geram efeitos bem claros e visíveis na estrutura política mundial, tornaram-se uma tendência em crescimento nas últimas décadas e suas particularidades demandam atenção. Entre outros, as restrições em termos 'deterrence' e a grande facilidade de atuação tanto para indivíduos quanto para os Estados colocam em questão os paradigmas até então utilizados para orientar os estudos sobre o tema e inspiram novas pesquisas. Este trabalho tem o objetivo de demonstrar a efetividade dos ciberataques e da guerra cibernética, seja ela explícita ou não, para a obtenção de poder no cenário internacional, além de apresentar dois estudos de casos ocorridos na primeira década do século XXI.

Palavras-chave: tecnologia da informação e comunicação, ciberconflitos, ciberataques, ciberespaço, relações internacionais, segurança internacional.

The usage of Cyberspace to attain power during the early twenty-first century

ABSTRACT

There's no doubt about the importance of the cyberspace to the current society, not only because of the fast development of the cyberculture, but also for its mandatory presence on everyday business and government activities. However, its increasing usage and the large possibilities it opens to different actors bring new challenges in terms of governance and security. The military operations whithin the cyberspace, often cloaked in secrecy but generating clear effects on the international politics, became a strong tendency in the last decades and demand attention. Moreover, the cyberspace is a totally new environment, with new peculiarities, and its restrictions to the traditional deterrence and ease of action to several actors, ranging from individuals to States, raise questions about the capability of the usual paradigms of analysis in yelding reliable conclusions. This work intends to show how cyberattacks are effective to attain power in the international scene. It also presents two case studies of international cyber attacks that happened in the first decade of the XXIst century.

Keywords: communication and information technology, cyberconflicts, cyberattacks, cyberspace, international relations, international security

LISTA DE FIGURAS

Figura 1 - Tipos de Conflito no Ciberespaço 14
Figura 2 - Buscas realizadas no período de 2004 a 2017 para o termo 'cyber warfare' na ferramenta de pesquisa da empresa 'Google' 29

LISTA DE QUADROS

Quadro 1 - Dimensões física e virtual do poder cibernético 47
Quadro 2 - As três faces do poder no domínio cibernético 47
Quadro 3 - Os atores e suas fontes de poder no Ciberespaço 48

LISTA DE SIGLAS E ABREVIATURAS

CIA - '*Central Intelligence Agency'* ou Agência Central de Inteligência
CSNU - Conselho de Segurança das Nações Unidas
DIA - '*Defense Intelligence Agency'* ou Agência para Inteligência de Defesa
DDoS - '*Distributed Denial of Service'* ou Negação de Serviço Distribuída
EUA - Estados Unidos da América
FBI - '*Federal Bureau of Investigation'* ou Serviço Federal de Investigação
GPS - *'Global Positioning System'* ou Sistema de Posicionamento Global
INTERPOL - '*International Criminal Police Organization' ou Organização Internacional de Polícia Criminal*
KGB - '*Komitet Gosudarstvennoje Bezopasnoti'* ou Comitê de Segurança do Estado
MIT - '*Massachusetts Institute of Technology'* ou Instituto de Tecnologia de Massachusetts
Mossad - Serviço Secreto Israelense
NSA - *National Security Agency* ou Agência de Segurança Nacional
NYT - '*The New York Times*', Jornal estadunidense de tendência democrata
O.I. - Organizações Internacionais
OCDE - Organização para a Cooperação e o Desenvolvimento Econômico
OEA - União dos Estados Americanos
OTAN - Organização do Tratado do Atlântico Norte
SCADA - Sistema de Controle Industrial
TCP-IP - '*Transmission Control Protocol'* ou Protocolo para Controle de Transmissão
UE - União Europeia
URSS - União das Repúblicas Socialistas Soviéticas
WWW - '*World Wide Web*', rede de comunicação internacional operando sobre o protocolo HTTP

SUMÁRIO

INTRODUÇÃO **1**

CAPÍTULO I - DEFINIÇÃO DOS CONCEITOS BÁSICOS

1.1. Introdução 5
1.2. O Ciberespaço 6
1.3. A Estrutura do Ciberespaço 6
1.4. A Internet 8
1.5. Os Ciberataques e a Guerra Cibernética 9

CAPÍTULO II - O CIBERESPAÇO COMO UM INSTRUMENTO DE PODER

2.1. Introdução 17
2.2. Os Conflitos Cibernéticos e as Teorias de Relações Internacionais 17
a) Idealismo 18
b) Realismo 26
c) Neoliberalismo 31
2.3. O Poder Cibernético na Visão de Joseph Nye Jr. 41

CAPÍTULO III - ESTUDO DE CASO: GEÓRGIA

3.1. Introdução 53
3.2. O Conflito 55
3.3. Conclusão 61

CAPÍTULO IV - ESTUDO DE CASO: STUXNET

4.1. Antecedentes 65
4.2. Um novo tipo de arma cibernética 67
4.3. O Ataque. 70
4.4. Conclusão 75

CONSIDERAÇÕES FINAIS **78**
REFERÊNCIAS BIBLIOGRÁFICAS **81**

INTRODUÇÃO

INTRODUÇÃO

É inegável que os sistemas computadorizados de informação e suas estruturas de conexão, as redes de computadores, são imprescindíveis para o funcionamento do mundo atual. A enorme velocidade com que estes sistemas eletrônicos permitem a troca e o processamento de informações, aliada à facilidade de interação que oferecem aos seus usuários onde quer que eles estejam no planeta, gerou muitas mudanças para a sociedade durante as últimas décadas, e possibilitou novas visões de mundo que afetaram e continuam afetando comportamentos e relações interpessoais e coletivas. Este novo paradigma de organização social foi chamado de "Era da Informação" e se caracteriza pela transformação do modo de vida baseado em tecnologias mecânicas oriundas da revolução industrial para o uso intenso da informação eletrônica e computadorizada (HILBERT, 2016).

A última década do século XX e as primeiras décadas do século XXI marcam o início da "Era da Informação", as novas possibilidades que ela representa para a humanidade envolvem mudanças profundas através de uma "grande proliferação de tecnologias e capacidades emergentes de informação e comunicação que possibilitarão à humanidade superar as barreiras de interação impostas pelo tempo, distância e localização, além de ampliar a capacidade de processar informações e tomar decisões" (ALBERTS; PAPP, 1997, pg 13)[1] Se colocarmos esta afirmação sob uma perspectiva quantitativa, os números não deixarão nenhuma dúvida sobre a velocidade e intensidade deste fenômeno:

> Há apenas uma geração atrás a internet era nada mais do que uma conexão eletrônica entre uns poucos pesquisadores universitários. O primeiro "correio eletrônico" [chamado *e-mail*] foi enviado em 1971. Os filhos destes cientistas hoje vivem num mundo onde 40 trilhões de *e-mails* são enviados por ano. O primeiro *website* [página eletrônica na internet] foi criado em 1991. Em 2013, já havia cerca de 30 trilhões de páginas individuais na internet. (Singer e Friedman, 2014, pg 2)[2]

A internet, que foi inicialmente imaginada por J. C. R. Licklider do MIT em 1962 como "um conjunto mundial de computadores interconectados através dos quais

[1] tradução nossa, do original: "widespread proliferation of emerging information and communication technologies and the capabilities that those technologies provide and will provide humankind to overcome the barriers imposed on communications by time, distance, and location and the limits and constraints inherent in human capacities to process information and make decisions."

[2] tradução nossa, do original: "Just a generation ago, the Internet was little more than a link between a few university researchers. The first “electronic mail” was sent in 1971. The children of those scientists now live in a world where almost 40 trillion e-mails are sent a year. The first “website” was made in 1991. By 2013, there were over 30 trillion individual web pages."

qualquer pessoa pudesse rapidamente acessar dados e programas onde quer que estivesse" (Internet Society, 2016)[3], se tornou o principal meio e, ao mesmo tempo, o principal catalizador destas mudanças. Na década de 1990, quando esta rede mundial de intercomunicação ainda estava no seu começo, a percepção do seu impacto já era clara:

> A revolução começa quando esses computadores conectam-se uns ao outros. Dois em cada cinco computadores nos EUA já fazem parte de uma rede - a maioria dentro de empresas -, mas muitos já estão cruzando estes limites, a medida que a tecnologia de interconexão progride.
> (Alberts e Papp, 1997, pg 8)[4]

Atualmente é raro encontrar um computador que não esteja conectado à internet. O ambiente *online* deixou de ser uma opção e tornou-se uma necessidade. Isto porque o intenso uso de softwares no dia a dia das pessoas, indo desde a escrita de um texto até a execução de cálculos e atividades complexas, passando pela leitura das notícias diárias e controle da agenda pessoal, modificou a maneira como as tarefas diárias são realizadas, criando facilidades e, ao mesmo tempo, novas possibilidades. A intercomunicação à distância passou a nos acompanhar o tempo todo em computadores de bolso ("smartphones") e até mesmo nos equipamentos associados às atividades mais triviais, como pegar dinheiro no banco (caixas eletrônicos) e assistir televisão (TVs a cabo e TV digital). O uso da internet passou a permear quase todas as atividades do cidadão moderno:

> A internet não se restringe mais ao envio de "e-mails" e à troca de informações: ela agora abrange tudo o que nos cerca indo desde usinas de geração de energia ao rastreamento das compras de bonecas Barbie. De fato a Cisco, uma empresa responsável por grande parte dos sistemas eletrônicos que compõem a parte física da internet, estima que de 8.7 milhões de equipamentos conectados à internet no final do ano 2012 passaremos a cerca de 40 milhões por volta de 2020; quando carros, frigideiras, equipamentos médicos e aparelhos ainda não inventados começarão também a funcionar conectados à internet. (Singer e Friedman, 2014, pg 2)[5]

[3] tradução nossa, do original: "globally interconnected set of computers through which everyone could quickly access data and programs from any site."

[4] tradução nossa, do original: "The revolution begins when these computers hook up to one another. Already two out of five computers in the U.S. are part of a network —mostly intracompany nets, but more and more are crossing company lines, just as InterDesign's electronic data interchange does. Data traffic over phone wires is growing 30 percent a year, says Danielle Danese, a telecommunications analyst at Salomon Brothers. Traffic on the global Internet doubles every year."

[5] tradução nossa, do original: "Internet is no longer just about sending mail or compiling information: it now also handles everything from linking electrical plants to tracking purchases of Barbie dolls. Indeed, Cisco, a company that helps run much of the back end of the Internet, estimated that 8.7 billion devices were connected to the Internet by the end of 2012, a fi gure it believes will rise to 40 billion by 2020 as cars, fridges, medical devices, and gadgets not yet imagined or invented all link in."

Estes números, demonstrando a intensidade das transformações em curso, impressionam mas há também um outro lado: ao mesmo tempo em que todas estas possibilidades e facilidades crescentes representam benefícios para os cidadãos em geral, elas também podem significar ameaças se utilizadas por pessoas ou até mesmo governos mal intencionados. Dentro deste contexto, o uso dos recursos de comunicação eletrônica e da internet para fins ilícitos e para a obtenção de vantagens que até então eram difíceis ou impossíveis de se obter de outra maneira, tornou-se um grande perigo para todas as sociedades envolvidas com a "Era da Informação".

> Há uma piada antiga das empresas de segurança sobre como proteger um computador: "Simplesmente desconecte-o". O problema é que, não só esta piada está se tornando anacrônica numa era de aparelhos sem fio portáteis, mas também que, mesmo conectado, há muitas maneiras de desviar o uso das finalidades propostas para um equipamento eletrônico. Este desvio [de função] é chamado mal funcionamento. E quando a diferença entre o funcionamento esperado e o atual é causada por má fé (não um simples erro ou acidente), então este mal funcionamento se torna um problema de segurança. (Singer e Friedman, 2014, pg 34)[6]

Considerando-se que a tecnologia é uma ferramenta, e como tal pode ser utilizada tanto para o bem quanto para o mal, é possível perceber então como a informação intermediada pela tecnologia moderna, com todo o seu poder transformador social, também pode ser utilizada como uma arma, a serviço de interesses escusos e perniciosos a determinados Estados, indivíduos ou à sociedade em geral.

O objetivo deste trabalho é demonstrar que o ciberespaço (compreendendo a internet e os diversos equipamentos de comunicação eletrônica digital interconectados a nível global) tem sido utilizado por alguns países para a obtenção de poder no cenário internacional. Foram pesquisados casos de ataques cibernéticos bem documentados em livros, jornais e revistas que permitem estabelecer um elo claro de interesse circunstancial entre os países suspeitos de perpetrar o ato e os resultados do ataque. Se as consequências políticas destes ataques nos países vitimados realmente caracterizarem um efeito coercitivo favorecendo os interesses dos supostos atacantes, confirmar-se-á o ciberespaço como um novo ambiente capaz de afetar o equilíbrio de forças mundial.

[6] tradução nossa, do original: " There's an old joke in the security industry about how to secure any computer: Just unplug it. The problem is not only that the joke is becoming outdated in an era of wireless and rechargeable devices, but once a machine is plugged in, there are practically an infinite number of ways its use might deviate from its intended purpose. This deviation is a malfunction. When the difference between the expected behavior and actual behavior is caused by an adversary (as opposed to simple error or accident), then the malfunction is a "security" problem."

A monografia está organizada da seguinte maneira: o capítulo 1, "Definição de Conceitos Básicos", visa explicar os marcos conceituais e as nomenclaturas características ao tema. Termos como ciberespaço, ciberguerra e outros são definidos para permitir a compreensão adequada do embasamento teórico posteriormente utilizado neste trabalho. No capítulo 2, "O Ciberespaço como um Instrumento de Poder", são exploradas possibilidades de análise dos conflitos de poder no domínio cibernético a partir de algumas das principais teorias políticas de relações internacionais e apresentado o referencial teórico escolhido para o estudo do exercício de poder neste meio, a visão neoliberal de Nye Jr.; fornecendo assim subsídios para as análises, realizadas nos últimos capítulos, de dois episódios marcantes de ciberconflitos ocorridos no início do século XXI.

CAPÍTULO I

DEFINIÇÃO DOS CONCEITOS BÁSICOS

1.1 Introdução

Temos observado um crescimento significativo nestas últimas décadas na quantidade de trabalhos sobre o ciberespaço dentro do contexto das relações internacionais. Entretanto, como se trata de um tema multidisciplinar, muitas vezes os conceitos e os termos técnicos envolvidos não são utilizados ou compreendidos com a devida precisão, o que pode não só causar confusão mas também, ainda pior, impedir o desenvolvimento de conclusões realmente significativas. Este capítulo tem o objetivo de esclarecer os conceitos mais importantes para a compreensão das ideias aqui apresentadas.

1.2 O Ciberespaço

A palavra "ciberespaço" (do inglês *cyberspace*) apareceu inicialmente num romance de ficção científica chamado *neuromancer*, do escritor americano-canadense William Gibson, e foi utilizada para designar uma "alucinação consensual" entre os personagens (Kuehl, 2009, p. 25). A partir da década de 1990, com a rápida evolução e ampliação da comunicação via rede de computadores, de maneira que seus usuários passaram a reconhecê-la como um novo tipo de ambiente para a interação interpessoal, o termo começou a ser utilizado como uma maneira de diferenciá-la da experiência de comunicação à distância obtida através de outros dispositivos (Strate, 1999). Entretanto, ainda não havia uma definição precisa para o termo ciberespaço e esta somente começou a ser construída quando houve a necessidade de se implantar políticas públicas para lidar com os problemas de segurança que este novo ambiente trazia. Na primeira década do século XXI o Departamento de Defesa estadunidense editou diversos documentos nos quais apresentava definições cada vez mais elaboradas para a ideia de ciberespaço sem, no entanto, conseguir compor um texto que fosse, ao mesmo tempo, abrangente e preciso (Kramer, 2009). Encontramos em Kuehl (2009, p. 29) uma definição que tem sido bem aceita pelos trabalhos acadêmicos consultados: o ciberespaço é "um domínio global dentro do ambiente de troca de informações cuja característica única e distintiva é utilizar-se da eletrônica e do espectro eletromagnético para criar, armazenar, modificar, trocar e processar informações via redes interconectadas e interdependentes usando tecnologias de informação e comunicação"1. Ou seja: o

ciberespaço abrange não só os computadores e suas redes de conexão mas também todo o equipamento eletrônico capaz de se comunicar com estas redes e com elas trocar informações. Neste sentido podemos perceber então que o rádio, telégrafo, sistemas de telefonia móvel/fixa, televisão digital, entre outros, também fazem parte do ciberespaço. E o motivo desta considerável abrangência da definição apresentada é a tendência, cada vez mais intensa, de intercomunicação entre os equipamentos eletrônicos mais diversos, e deles com as grandes redes computadorizadas de troca de informação, compondo assim o grande sistema dinâmico e altamente diversificado que é chamado de ciberespaço.

1.3 A Estrutura do Ciberespaço

A compreensão básica do funcionamento do ciberespaço é importante para a discussão em questão e para isto apresentaremos uma estrutura resumida por camadas lógicas, de maneira que possamos distinguir conceitualmente os elementos mais importantes deste grande sistema sem que seja necessário adentrar em detalhes técnicos. Dividiremos o ciberespaço em três camadas principais: uma mais superior, composta pela informação que será transmitida; outra intermediária, composta pelos recursos lógicos (softwares) que transformam a informação em códigos compreensíveis pela máquina; e outra mais inferior, composta pelos equipamentos e cabos (hardware) que transformam os códigos em sinais elétricos e os transmitem. A camada superior se constitui na informação propriamente dita, fornecida pelo usuário, que é transformada em padrões (caracteres) e comandos compreensíveis pelo computador através de um recurso lógico chamado protocolo (software). O protocolo, por sua vez, controla os níveis intermediários de codificação que irão transformar os caracteres em padrões de sinais elétricos, de maneira que eles possam ser transmitidos através dos cabos de rede (ou por via aérea, através de sinais eletromagnéticos de rádio) até o receptor. Uma vez chegando ao receptor, os sinais elétricos serão decodificados novamente em códigos pelo nível intermediário até chegar ao protocolo quando, finalmente, são retransformados em informação e reconhecidos pelo usuário (Singer; Friedman, 2014, p. 23).

Estes diversos níveis de codificação são necessários porque a linguagem humana não é compreendida pelas máquinas e cada nível de interação com os

[1] tradução nossa, do original: "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."

sistemas eletrônicos possui um tipo de específico de codificação: o protocolo reconhece somente caracteres e os circuitos e cabos de transmissão reconhecem somente sinais elétricos (Ceruzzi, 2003, p. 93).

> Uma outra maneira de se representar o ciberespaço é através de múltiplas camadas. A fundação se constitui num grupo de recursos físicos que fornecem a estrutura tangível através da qual as pessoas acessam e usam o ciberespaço. O próximo nível se consiste nas plataformas e sistemas tecnológicos que são utilizados para criar, armazenar, modificar, trocar e processar a informação de inúmeras maneiras. É neste nível que nós planejamos e construímos o ciberespaço, porque cada um destes ciberrecursos [software] é voltado para um fim específico, e nós os combinamos para criar sistemas e redes ainda mais complexos. O outro nível é a informação propriamente dita (Kuehl, 2009, p. 33)[2]

Podemos observar então que existem pelo menos duas grandes estruturas básicas de funcionamento no ciberespaço: a estrutura física (chamada hardware), composta por cabos e equipamentos eletrônicos que processam e transmitem a informação, e a estrutura lógica (chamada software), que codifica e decodifica a informação em variações elétricas compreensíveis pela máquina. A percepção destas estruturas é importante porque elas definem dois tipos diferentes de intervenção no ciberespaço: a intervenção física, que age sobre os equipamentos, computadores e os cabos de transmissão; e a intervenção lógica, que acontece através de linguagens de programação específicas. Embora um nível seja bem diferente do outro, eles estão interconectados de maneira que recursos ou equipamentos físicos podem ser controlados remotamente por softwares específicos e vice-versa.

> A dimensão física interconectada [à dimensão lógica] é a maneira mais básica pela qual o ciberespaço realiza a transmissão de informações, porque os recursos tecnológicos de um mundo interconectado são dominados pelo ciberespaço (Kuehl, 2009, p. 32)[3]

1.4 A internet

O ciberespaço é composto por inúmeras redes interconectadas e a maior de todas, que realiza a interconexão de todas as redes menores, é a internet (SINGER;

[2]tradução nossa, do original: "Another way of looking at this is to portray cyberspace as having multiple layers. At the foundation is the set of physical characteristics that create the basic frameworks of how we enter and use cyberspace. The next layer consists of the platforms and technological systems that we create and employ to create, store, modify, exchange, and exploit information in all its myriad forms. This is where we design and build cyberspace, because each of these cyber platforms is created with a purpose, and we combine them to create even newer and more complex/capable systems and networks. The next layer is the information itself."

[3]tradução nossa, do original: "the physical/interconnected dimension, is the primary means by which cyberspace touches and shapes the information environment, because the technological aspects of an interconnected world are dominated by cyberspace."

FRIEDMAN, 2014, p. 21). Ou seja: o ciberespaço é uma superestrutura bem mais ampla do que a internet, abrangendo praticamente todos os meios de comunicação eletrônica utilizados hoje em dia, e faz uso da internet para obter abrangência mundial, alcançando os pontos mais remotos do globo. A internet não deve ser confundida com o ciberespaço porque é apenas um dos muitos meios de transmissão eletrônica de dados existente, um intermediador da comunicação entre redes mais ou menos independentes, mas pode certamente ser considerada a mais importante destas redes, pelo seu papel centralizador, facilitador e disseminador da cultura digital. Afirma Ceruzzi (2003, p. 295) "A internet não é uma rede única mas sim um meio de conexão entre diferentes redes espalhadas pelo mundo, daí o seu nome."[4] A sua grande popularidade e aceitação pelos mais diferentes países e centros de pesquisa do mundo se deve a várias características bem específicas, entre elas o uso de padrões abertos, governança técnica participativa e neutralidade no tratamento de conteúdo, facilitando assim o seu crescimento entre as iniciativas privadas e públicas de diversos países e transformando-a na rede das redes (Kurbalija; Gelbstein, 2005).

1.5 Os Ciberataques e a Guerra Cibernética

A Era da Informação fez com que o ciberespaço e os seus desafios em termos de segurança recebessem uma grande atenção da sociedade em geral, gerando uma significativa quantidade de estudos especializados, como o de KUEHL (2009), CLARKE e KNAKE (2010), NYE JR (2011), entre vários outros. Entretanto, a rapidez com que este fenômeno evoluiu e continua evoluindo ainda não permitiu que os conceitos desenvolvidos, e até mesmo a nomenclatura mais básica utilizada para descrevê-lo, alcançassem um consenso. A natureza multifacetada do ciberespaço, interagindo simultaneamente com inúmeros aspectos diferentes da realidade social, e as diversas possibilidades de poder que surgem destes mesmos interrelacionamentos inspiram os mais variados tipos de interpretações e enfoques.

> [...] ciberespaço já está no nosso vocabulário há cerca de duas décadas, desde quando William Gibson utilizou este termo para descrever uma "alucinação consensual" no seu romance de ficção científica, 'Neuromancer'. Entretanto, ainda não há nenhum consenso sobre o que ele representa [para o mundo] neste início do século XXI. Ao mesmo tempo em que os órgãos governamentais tentam definir o que é o ciberespaço num

> aspecto mais prático, operacional - a definição de Gibson é obviamente insuficiente -, o tipo de compreensão que está sendo desenvolvida sobre este domínio irá definir como ele interagirá com os outros domínios [já existentes] e afetará suas relações com os outros elementos e instrumentos de poder, especialmente a maneira como os seres humanos e as organizações utilizam o poder que ele proporciona. (KUEHL, 2009, p. 1) [4]

Esta dificuldade de consenso, oriunda da multiplicidade de pontos de vista e abordagens distintas, se reflete claramente na nomenclatura escolhida por cada autor fazendo com que os termos escolhidos muitas vezes causem dúvidas ou confusão.

> Assim como acontece em qualquer nova área de estudos, não há consenso entre os pesquisadores sobre quais seriam os termos mais adequados a serem utilizados [em seus trabalhos], e por isso eles utilizam o tipo de vocabulário que entendem como mais representativo para o fenômeno abordado. Desta maneira, devido à grande diversidade de possiblidades descritivas, este campo de estudos tem conhecido uma abundância de termos e ideias concorrentes. Conceitos como 'revolução em assuntos militares', 'guerra de quarta geração', 'guerra eletrônica', 'guerra de informação', 'guerra em rede' e 'guerra cibernética' têm sido oferecidos para explicar o surgimento desta nova área de conflitos [...] (GREATHOUSE, 2014, p. 23) [5]

E dentre estes, o termo 'guerra cibernética' é o mais propenso à polêmica pois tem sido empregado com significados diferentes por vários autores dentro do mundo acadêmico, além de apresentar conotações ainda mais diversificadas na mídia e na compreensão popular.

> [...] O termo 'guerra cibernética' tem sido usado com uma frequência cada vez maior na mídia e também nas discussões políticas. Originalmente este termo foi cunhado junto com o seu análogo 'guerra em rede' [*netwar*] no início dos anos 1990 para identificar um novo conjunto de técnicas operacionais e o novo modo de se fazer guerra que estava surgindo na Era da Informação. Desde então ambos os termos se tornaram parte do linguajar oficial das operações militares relacionadas com a tecnologia da informação nos EUA. Mas o termo 'guerra cibernética' acabou ganhando

4 tradução nossa, do original: "[...] Cyberspace has been in our lexicon for two decades, since William Gibson used it to describe “a consensual hallucination” in his science fiction novel, Neuromancer, but there certainly is no consensus on its meaning in the world of the 21st century. While organs of government attempt to define its meaning in the real, operational world - Gibson’s approach obviously will not suffice - the approaches we develop toward this domain will shape how it interacts with other domains and affects relationships among the other elements and instruments of power, especially how humans and the organizations we create use that power."

5 tradução nossa, do original: "As with any emerging area of study there's no commonaly whithin the field about the correct terms which should be used. Authors can and do create language which they fell enable to best describe the phenomena they are trying to address. However, because of the diversity of descriptions offered, the field has quickly become overrun with competing ideas and terms. Concepts such as the revolution in military affairs (RMA), fourth generation warfare, electronic warfare, information warfare, network centric warfare, and cyber war have all been offered to explain the emerging area of conflict [...]"

> uma grande variedade de conotações fora dos círculos militares. O seu uso popular tem se referido ultimamente a qualquer tipo de fenômeno envolvendo ações destrutivas ou interruptivas em sistemas computacionais, o que levou o responsável pela segurança cibernética dos EUA durante o governo Obama, Howard Schmidt, a chamá-lo de 'uma metáfora infeliz' (CAVELTY, 2012, p. 111) [6]

Entretanto, a compreensão do que seria uma 'guerra cibernética' e sua relação com os diversos tipos de ataques cibernéticos (ciberataques) é de grande importância para este trabalho e por isso faremos uma breve exposição sobre como o termo é interpretado por alguns dos principais autores nesta área de estudo e ao final apresentaremos a uma definição mais ampla capaz de amparar as análises aqui desenvolvidas.

Numa abordagem realista, CLARKE e KNAKE (2010) enfatizam a visão militar do termo dentro de uma perspectiva estadocêntrica para os atores. E como exemplo para a definição apresentada citam a "Operação Pomar", realizada em 2007 por Israel com o objetivo de destruir instalações nucleares que, na época, estavam sendo construídas pela Síria (Associated Press, 2011). O ataque fez uso de vários caças bombardeiros F-16 que não foram detectados pelas forças antiaéreas sírias devido a uma intervenção cibernética previamente realizada pelos israelenses nos sistemas de controle dos radares (HERSH, 2008).

> [...] ['guerra cibernética] se refere a ações realizadas por Nações ou Estados para penetrar as redes ou computadores de outras Nações com o propósito de causar dano ou interrupção [no funcionamento de sistemas eletrônicos]. Quando os israelenses atacaram a Síria eles utilizaram luz e pulsos elétricos não para cortar [objetos] como faz uma arma LASER ou para atordoar pessoas tal qual um TASER, mas sim para transmitir 'zeros' e 'uns' [através de redes de computadores] e desta maneira controlar o que os radares da defesa aérea síria estavam vendo. Ao invés de explodir o sistema de defesa aérea sírio e assim perder a vantagem do elemento surpresa bem antes de atingir o seu alvo principal, na era da 'guerra cibernética' os israelenses conseguiram garantir que o inimigo não fosse capaz nem mesmo de ativar as suas defesas. (CLARKE; KNAKE, 2010, p. 11) [7]

6 tradução nossa, do original: "[...] the term ‘cyber war’ is used more and more frequently in the media but also in policy circles. Originally, the term was coined together with its twin concept ‘netwar’ in the early 1990s to signify a set of new operational techniques and a new mode of warfare in the information age. Both have since become part of official (US) military information operations doctrine in modified form. But ‘cyber war’ also leads a colourful life outside the military discourse: The popular usage of the word has come to refer to basically any phenomenon involving a deliberate disruptive or destructive use of computers, which has prompted US President Barack Obama’s cyber security czar Howard Schmidt to repeatedly call it a ‘terrible metaphor’."

7 tradução nossa, do original: "[...] it refers to actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption. When the Israelis attacked Syria, they used light and electric pulses, not to cut like a laser or stun like a taser, but to transmit 1’s and 0’s to control what the Syrian air defense radars saw. Instead of blowing up air defense radars and giving up the element of surprise before hitting the main targets, in the age of cyber war, the Israelis ensured that the enemy could not even raise its defenses."

Ainda nesta perspectiva estadocêntrica para os atores, a definição apresentada por SCHAAP (2009), num trabalho divulgado pela força aérea estadunidense, retira o foco do ato de agressão e enfatiza a manipulação das informações transmitidas pela rede do país atacado, demonstrando assim um ponto de vista mais técnico dentro da área de informática. Os militares veem um ataque como uma forma de causar danos perceptíveis ao inimigo, mas em informática este dano pode ser sutil e não acontecer em meio físico (pelo menos num primeiro momento), mas sim através da apropriação ou destruição de informações importantes.

> O uso de recursos em rede de um Estado por um outro Estado visando interromper, negar, debilitar, manipular ou destruir informações localizadas em computadores ou rede de computadores, ou os próprios computadores e redes. (SCHAAP, 2009, p. 127) [8]

A visão militar do fenômeno, estadocêntrica e bastante influenciada pela guerra tradicional, atinge o seu ápice num estudo realizado pela ONU que contou com diversos especialistas em direito internacional, além de militares e consultores diversos. Neste trabalho o ciberataque é entendido como o ato que perpetra a guerra cibernética e, sem apresentar uma definição para a guerra em si, define somente o ato de agressão cibernético:

> Um ciberataque é uma operação realizada no ciberespaço, com natureza ofensiva ou defensiva, que, numa avaliação razoável, é considerada capaz de causar ferimentos ou morte às pessoas, ou danos ou destruição aos objetos (SCHMITT, 2013, p. 106) [9]

Entretanto, esta visão militar não se mostra capaz de explicar ou abranger todas as possibilidades de manifestação perniciosa dentro do ciberespaço, e isto acontece por vários motivos:

a) não é possível pensar um ataque cibernético somente como sendo um ato de Estado porque a internet e o ciberespaço em geral permitem que vários atores diferentes, desde uma pessoa comum até empresas ou organizações em geral, realizem, de maneira coordenada ou não, atos capazes de prejudicar alvos variados que também vão desde outras pessoas comuns até Estados, passando por empresas e organizações em geral.

8 tradução nossa, do original: "The use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves, of another state."

9 tradução nossa, do original: "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects"

b) é importante notar que o custo extremamente baixo de um ataque cibernético (muitas vezes envolvendo apenas o uso de um microcomputador com acesso à internet) não se compara ao custo de uma guerra tradicional que envolve aviões, navios, soldados, força terrestre, etc. A consequência deste fato é que os ataques cibernéticos podem acontecer continuamente por vários anos (muitas vezes sem que a vítima os perceba) e têm grandes facilidades para ocultação da sua origem (porque há muitos outros computadores disponíveis na rede cujo funcionamento pode ser alterado para que ajam como "intermediários" ou "marionetes"). Por outro lado, um ataque militar tradicional tem o seu responsável e o seu momento claramente definidos no tempo e no espaço, e os seus recursos rapidamente esgotados na intensidade da batalha.

c) o foco primário dos ataques cibernéticos não são pessoas ou objetos, mas sim informações de alguma forma acessíveis através das redes de computadores, sejam elas privadas ou públicas.

A partir destas observações é possível compreender que uma 'guerra cibernética' pode acontecer de maneira silenciosa e prolongada através, por exemplo, do roubo de informações militares sensíveis, da manipulação remota de redes digitais que fazem o controle de sistemas militares ou instalações industriais, obtenção de códigos e senhas secretas que dão acesso a recursos de alto impacto para a sociedade, etc. E também, num tipo diferente de ataque cibernético, pode afetar indiretamente recursos físicos, danificando outros computadores ou redes e até mesmo realizando a transferência eletrônica de fundos entre contas bancárias, além de outras possibilidades.

Pensando nesta natureza multifacetada dos ciberataques, mas sem definir com clareza o que seria uma guerra em meio digital, NYE JR, falando a partir da sua visão neoliberal, muda o paradigma de abordagem da questão ao propor uma perspectiva bem mais ampla no que se refere a atores e possibilidades de ataques.

> Um conflito extremo dentro do domínio cibernético, uma 'guerra cibernética', é também algo diferente. No mundo físico os governos têm o monopólio do uso da força em larga escala, os defensores possuem um profundo conhecimento do terreno e os ataques terminam por atrito ou exaustão. Tanto os recursos quanto a mobilidade representam um alto custo. No mundo virtual os atores são diversificados, muitas vezes anônimos, a distância física é desprezível e um ataque simples possui custo quase nulo [...] (NYE JR, 2011, p. 5) [10]

10 tradução nossa, do original: "Extreme conflict in the cyber domain or “cyber war” is also different. In the physical world, governments have a near monopoly on large scale use of force, the defender has an intimate knowledge of the terrain, and attacks end because of attrition or exhaustion. Both resources and mobility are costly. In the virtual world, actors are diverse, sometimes anonymous, physical distance is immaterial, and a single virtual offense is almost cost free. [...]"

Percebe-se então que, para uma correta definição do termo 'guerra cibernética', é necessário uma percepção mais detalhada dos tipos de ciberataques, suas naturezas e contextualizações.

> O termo 'guerra cibernética' cobre apenas uma pequena parte dos ciberataques. Do ponto de vista militar ele deveria ser considerado como parte da 'guerra de informação' e, para que seja possível determinar a sua natureza e relevância, nós necessitamos não só uma definição léxica clara mas também uma diferenciação entre as dimensões estratégicas e operacionais de uma 'guerra cibernética' [...] (CAVELTY, 2010) [11]

Neste sentido, o Centro de Estudos de Segurança sediado em Zurique publicou um trabalho (CAVELTY, 2010) propondo a utilização do termo 'conflito' (que representa oposição de interesses e pode compreender um ou vários ataques, simultâneos ou não) para, a partir dele, construir distinções representando as diversas possibilidades de agressão cibernética. E para que estas definições tenham um sentido prático nas análises, elas não devem se basear nos possíveis perpetradores do ato (já que estes normalmente são bem difíceis de serem identificados no ciberespaço) mas sim na provável intenção do ato (bem mais fácil de ser deduzida através do contexto do ataque e dos danos causados).

> Na prática está se tornando cada vez mais difícil categorizar os ciberataques a partir dos seus perpetradores. Uma vez que a capacidade de ocultação dos responsáveis tem aumentado significativamente no ciberespaço, normalmente é impossível identificá-los de imediato. Entretanto, a intenção do ataque, na medida em que possa ser reconhecida com clareza, é de grande importância conceitual porque nem todo ciberataque tem origem militar ou faz parte de uma 'guerra cibernética'. Uma outra importante característica a ser levada em conta é o dano potencial causado pelo incidente [...] (CAVELTY, 2010) [12]

Desta forma a pesquisadora definiu 5 tipos de conflitos cibernéticos e os classificou em ordem crescente, criando assim uma 'escada de conflitos' que ascende segundo a intensidade e extensão dos danos potencialmente capazes de serem infligidos às suas vítimas.

11 tradução nossa, do original: "The term “cyberwar” only covers a narrow sub-section of all cyberattacks. From a military point of view, it should be regarded as part of information warfare. In order to determine the substance and relevance of the concept of “cyberwar”, we require not only a lexical definition, but also a differentiation between the operative and strategic dimensions of cyberwar [...]"

12 tradução nossa, do original: "In practice, it is becoming increasingly difficult to categorise cyberattacks primarily according to the perpetrators involved. Since the ability of attackers to conceal themselves is constantly improving, it is often impossible to identify them clearly and promptly. Nevertheless, the intention of an attack, as far as it can be established, is of conceptual importance, as by no means all cyberattacks have a military origin or are part of a cyberwar. Another important distinguishing feature is the potential damage caused by an incident. [...]

Figura 1 - Tipos de Conflito no Ciberespaço

Fonte: Cavelty, 2010.

Podemos observar na figura 1 que o conflito menos prejudicial seria o 'cibervandalismo', este que normalmente envolve um ou mais ataques visando modificar ou destruir o conteúdo de sites, mas cujos danos são normalmente reparados com rapidez e facilidade. A "escada" de conflitos sobe então num crescendo de conflitos e danos até chegar à 'guerra cibernética' que se consistiria num equivalente cibernético para a guerra tradicional, com grandes danos e prejuízos potenciais para uma ou mais partes envolvidas.

Segue uma definição detalhada para cada tipo de conflito apresentado na figura 1 (CAVELTY, 2010):

a) "Cibervandalismo": é o tipo mais comum de conflito e, de todos, o que causa menos danos. Se consiste em um ou mais ataques, simultâneos ou não, visando modificar ou destruir o conteúdo de sítios na internet ou fazer com que um computador servidor (responsável por manter um ou mais sítios disponíveis aos usuários) pare de funcionar por um determinado intervalo de tempo. Os efeitos deste tipo de ataque são bem definidos em termos de duração e conteúdo e, dependendo da competência dos responsáveis pelo sistema de manutenção, normalmente são contidos e superados com rapidez.

b) "Crime de internet": neste tipo de conflito o alvo quase sempre é o setor corporativo, e o grande objetivo dos ciberataques é o roubo de informações privilegiadas ou valorizadas no mercado negro digital, onde são posteriormente vendidas. Redes governamentais também são atacadas mas com menor frequência, devido ao alto investimento em conhecimento, preparação, tempo e dinheiro necessários para se penetrar em sistemas com níveis muito elevados de proteção, além da grande exposição obtida (perante os serviços secretos mundiais) ao se tentar vender este tipo de informação.

c) "Ciberespionagem": também é focado no setor corporativo (e evetualmente no setor público) mas acontece num nível bem mais sofisticado do que o "crime de

internet", tanto em termos de preparação quanto execução, porque visa a obtenção de dados sigilosos e segredos industriais, informações normalmente muito bem protegidas. Ciberataques deste tipo são capazes de causar danos significativos porque, quando realizados com sucesso, podem se manter de maneira continuada por largos períodos de tempo sem serem percebidos. A autora estima que o prejuízo anual total no mundo, somando-se os "crimes de internet" e a "ciberespionagem", chegue à ordem dos trilhões de dólares.

d) "Ciberterrorismo": se consiste em um ou vários ataques conduzidos por atores não governamentais e realizados com o objetivo de intimidar ou compelir um governo ou população a adotar um determinado comportamento. Pode ser perpetrado contra computadores, servidores ou redes governamentais e tem o potencial de causar grandes danos. Os ciberataques realizados contra a Georgia (descritos no capítulo 3), que foram oriundos de pequenos grupos e vários indivíduos supostamente incentivados pela Rússia (visando intimidar o governo local e facilitar os ataques físicos militares em andamento na fronteira), correspondem a este tipo de classificação.

e) "Guerra Cibernética": seria um tipo de conflito semelhante a uma guerra física, com atores estatais bem definidos, e cujo principal meio utilizado é o ciberespaço. Aqui o objetivo dos ataques é causar prejuízos físicos ou humanos ao inimigo, debilitando assim a sua capacidade de defesa e/ou ataque. Este tipo também engloba ataques cibernéticos visando facilitar ou viabilizar ataques físicos militares. Na prática, entretanto, o crescente uso de tecnologias digitais e eletrônicas nos combates militares já poderia ser considerada, pelo menos parcialmente, a realização deste conceito. A altíssima dependência que os sistemas militares atuais possuem dos recursos tecnológicos de ponta (comunicação via satélite, sistemas computadorizados para cálculo balístico e processamento de informações estratégicas, sistema de posicionamento avançado via rede de satélites, utilização cada vez mais maior de drones e mísseis teleguiados, etc) faz com que o ciberespaço se torne hoje em dia uma parte integrante e inalienável do mundo bélico. A "Operação Pomar" (HERSH, 2008), levada a cabo por Israel contra a Síria em 2007 e já descrita no início deste capítulo, seria um bom exemplo, mesmo que parcial, para a maneira como este tipo de conflito está se tornando cada vez mais presente.

Ao contrário das definições mais simples apresentadas no início deste capítulo, percebe-se que uma visão ampla, construída a partir da compreensão detalhada dos

tipos de ciberataques e suas motivações, permite não só vislumbrar uma distinção prática para os mesmos mas também definir de maneira efetiva o que seria a 'guerra cibernética', viabilizando assim uma análise mais consistente dos casos.

CAPÍTULO II

O CIBERESPAÇO COMO UM INSTRUMENTO DE PODER

2.1 Introdução

O capítulo anterior apresentou estudos demonstrando que o Ciberespaço é um novo domínio de poder cujos grandes desafios teóricos ainda estão longe de conhecer maiores consensos entre os pesquisadores. Entretanto, as teorias políticas já consolidadas no campo das Relações Internacionais nos permitem uma compreensão do tema sob perspectivas bem conhecidas e, contextualizadas no momento histórico das novas tecnologias, podem servir como uma visão preliminar sobre **o que o Ciberespaço representa em termos de conflito de poder**. Esta abordagem é apresentada no item 2.2. Também, considerando-se a diversidade de atores e possibilidades de intervenção observados no ambiente cibernético, a visão neoliberal de NYE JR nos proporciona uma análise mais ampla ao levar simultaneamente em consideração diversos elementos distintos sem perder de vista os aspectos político e militar do fenômeno, refletindo, desta maneira, boa parte da complexidade que envolve estas questões. A abordagem de NYE JR, explicando **como o poder pode ser efetivamente exercido no ciberepaço**, é apresentada no item 2.3.

2.2 Os Conflitos Cibernéticos e as Teorias de Relações Internacionais

A compreensão do que pode significar o Ciberespaço em termos de Relações Internacionais passa inevitavelmente pela confrontação das peculiaridades deste fenômeno mundial com algumas das principais teorias que embasam o campo de estudos. A utilização do arcabouço teórico já consagrado é essencial para que se possa definir uma abordagem de pesquisa tanto em termos de adequação ao tema quanto no que se refere às possibilidades epistemológicas.

> [...] é necessário estar familiarizado com a teoria porque os fatos não falam por si mesmos. Nós sempre olhamos para o mundo, seja de maneira consciente ou não, através de um conjunto específico de lentes; podemos chamar estas lentes de teoria [...] (JACKSON; SORENSEN, 2013, p. 57) [1]

Cada uma das principais teorias de Relações Internacionais foi construída sobre um ponto de vista específico que tenta explicar o funcionamento do sistema internacional e destaca, desta forma, componentes da realidade que podem ou não

1 tradução nossa, do original: "[...] It is necessary to be familiar with theory, because facts do not speak for themselves. We always look at the world, consciously or not, through a specific set of lenses; we may think of those lenses as theory [...]"

ser considerados significativos para a pesquisa desenvolvida.

> [...] [as teorias] nos mostram quais fatos são importantes ou não, ou seja: elas estruturam a nossa visão do mundo. As teorias são baseadas em determinados valores e quase sempre trazem consigo visões sobre como gostaríamos que o mundo fosse [...] (JACKSON; SORENSEN, 2013, p. 57) [2]

No que tange ao Ciberespaço foram escolhidas três correntes teóricas históricamente significativas para as transformações sofridas e os impactos causados por estas novas tecnologias que influenciaram sobremaneira o início do século XXI. São elas o Idealismo, Realismo e Neoliberalismo.

a) Idealismo

O final da Primeira Guerra Mundial é considerado um momento decisivo para os estudos de Relações Internacionais devido ao interesse que este grande conflito despertou para o problema das interações entre os Estados, terminando por transformar as Relações Internacionais num campo de estudos acadêmico independente. O enorme impacto emocional gerado pelos horrores da guerra e a quantidade nunca antes vista de vidas ceifadas em confrontos cada vez mais sangrentos, nos quais a mortandade foi muito intensificada pelo uso dos armamentos e das tecnologias de guerra do século XX, criou um sentimento generalizado na Europa de que aquela tragédia nunca mais deveria se repetir.

> O empurrão decisivo para a criação de um campo de estudos acadêmico independente e dedicado às Relações Internacionais foi dado pela Primeira Guerra Mundial (1914-18), que causou milhões de mortes. Ele surgiu da determinação generalizada de nunca mais se permitir que um sofrimento humano daquela intensidade acontecesse de novo [...] (JACKSON; SORENSEN, 2013, p. 34) [3]

E o fato dos EUA terem sido imprescindíveis para que o defecho do conflito fosse favorável aos aliados conferiu ao então presidente deste país, Woodrow Wilson, uma preponderância natural nos debates que aconteceram durante e após a grande guerra, tendo em vista a construção de um novo mundo onde um cataclisma daquele porte não tivesse mais razões para acontecer. As suas ideias para garantir a coexistência pacífica internacional, com a democracia prosperando entre

2 tradução nossa, do original: "[...] tell us which facts are important and which are unimportant, that is, they structure our view of the world. They are based on certain values, and often they also contain visions of how we want the world to be [...]"

3 tradução nossa, do original: "The decisive push to set up a separate academic subject of IR was occasioned by the First World War (1914–18), which produced millions of casualties; it was driven by a widely felt determination never to allow human suffering on such a scale to happen again [...]"

as nações, foram resumidas num programa de 14 pontos apresentado ao Congresso estadunidense em janeiro de 1918, iniciativa que lhe proporcionou o prêmio nobel da paz no ano seguinte.

> Os EUA foram finalmente levados à guerra em 1917. E a sua intervenção militar na Europa foi decisiva para o resultado do conflito: garantiu a vitória dos aliados democráticos (EUA, Grã Bretanha e França) e a derrota das potência autocráticas centrais (Alemanha, Austria e Turquia). Naquela época os EUA tinham um presidente, Woodrow Wilson, que fora professor de ciência política e que considerava como a sua principal missão levar valores liberais e democráticos para a Europa e o resto do mundo. Somente desta maneira, ele acreditava, uma outra grande guerra poderia ser evitada [...] (JACKSON; SORENSEN, 2013, p. 36) [4]

A disposição pacifista da opinião pública após a grande guerra e a crença de Wilson nos valores democráticos, além do seu empenho em propagá-los pelo mundo, fez com que a primeira grande corrente de pensamento de Relações Internacionais, chamada de "Liberalismo Utópico" (JACKSON; SORENSEN, 2013, p. 34) ou "Idealismo" (WEBER, 2010, p. 38), estivesse embasada na visão otimista de uma grande 'comunidade internacional', onde os conflitos poderiam ser superados através da colaboração mútua entre as nações. A ideia de que a ausência de um "governo mundial", capaz de impor a ordem entre as nações, era o motivo para as guerras perdeu força em favor do raciocínio de que a falta de comunicação adequada entre os países e a falta de incentivo às atitutes construtivas teriam levado à hecatombe.

> [...] a transformação da política internacional de conflituosa para cooperativa não exige um movimento da anarquia para a hierarquia, a transição de um sistema internacional sem uma autoridade superior para um sistema internacional submetido a um líder maior. Ao invés disso, tudo o que se necessita é a mediação e a substituição da anarquia pela [noção de] comunidade. Em outras palavras, um governo mundial pode não ser a única saída para a anarquia. A comunidade internacional, constituída por um conjunto de relações sociais coletivas de colaboração, tanto informais quanto formais, pode ser uma alternativa para um governo mundial ou uma anarquia internacional. (WEBER, 2010, p. 38) [5]

4 tradução nossa, do original: "The United States was eventually drawn into the war in 1917. Its military intervention decisively determined the outcome of the war: it guaranteed victory for the democratic allies (US, Britain, France) and defeat for the autocratic central powers (Germany, Austria, Turkey). At that time, the United States had a President, Woodrow Wilson, who had been a university professor of political science and who saw it as his main mission to bring liberal democratic values to Europe and to the rest of the world. Only in that way, he believed, could another great war be prevented [...]"

5 tradução nossa, do original: "[...] transforming international politics from conflictual to cooperative does not necessitate moving from anarchy to hierarchy, from an international system without an orderer to an international system with an orderer. Instead, all it requires is mediating or replacing anarchy with community. In other words, world government may not be the only way out of anarchy. International community, a formal or informal collective and cooperative set of social relationships among sovereign nation-states, may be an alternative to world government and an alternative to international anarchy."

O grande problema no sistema internacional, segundo os idealistas, seria a dificuldade de se promover uma comunicação adequada entre as nações, de maneira que um entendimento verdadeiro pudesse ser efetivamente construído.

> Se as pessoas pudessem ser organizadas de forma que a comunicação entre elas acontecesse de maneira verdadeira e honesta, elas perceberiam aquilo que possuem em comum e se uniriam em torno de padrões coletivos de bondade, verdade, beleza e justiça. Ou então (de uma maneira menos otimista) elas poderiam pelo menos elaborar regras ou leis que fossem capazes de amenizar os conflitos e facilitar a colaboração [...] (WEBER, 2010, p. 38) [6]

Embora este tipo de visão, considerada otimista demais, tenha sido abandonada a partir da década de 1930 com a ascensão do totalistarismo fascista, a Segunda Guerra Mundial em 1939 e o extenso período da Guerra Fria até a década de 1980; logo após a queda do muro de Berlim em 1989 e o fim do antagonismo entre EUA e URSS o mundo viveu novamente um período de confiança no futuro. As Teorias de Relações Internacionais em voga até então, como o neorealismo de Kenneth Waltz que explicava o sistema internacional através de uma competição constante por poder e um jogo de forças contrapostas, perderam a preponderância em favor do ressurgimento da visão idealista. E dentro desta perspectiva pacífica de compreensão do mundo "[...] um neoidealista em particular - Charles Kegley - chegou até a afirmar que o mundo pós-Guerra Fria se parecia muito com o mundo vislumbrado por Woodrow Wilson várias décadas antes [...]" (WEBER, 2010, p. 39) [7]

> [...] à medida em que a Guerra Fria arrefeceu durante a segunda metade da década de 1980 e o muro de Berlim foi derrubado em 1989, as verdades eternas de Waltz sobre competição, conflito e equilíbrio [de forças] num sistema de estrutura anárquica perderam a validade. A rivalidade entre leste e oeste acabou, acordos para controlar a proliferação de armas pareciam se proliferar mais rapidamente do que os armamentos, a democracia se espalhou pelo mundo e muitas Nações-Estado passaram a dar ênfase prática, não apenas retórica, aos direitos humanos e intervenções humanitárias [...] (WEBER, 2010, p. 39) [8]

6 tradução nossa, do original: "[...] If people could only be organized in ways that allow them to really, truly, and honestly communicate with one another, then they could see what they have in common and unite around common standards of goodness, truth, beauty, and justice. Or (somewhat less optimistically) they could at least put into place rules and laws to temper conflict and facilitate cooperation [...]"

7 tradução nossa, do original: "[...] One neoidealist scholar in particular - Charles Kegley - made the argument that the post-Cold War world looked very much like the world Woodrow Wilson envisioned decades before [...]"

8 tradução nossa, do original: "[...] as the Cold War thawed during the latter half of the 1980s and the Berlin Wall came down in 1989, Waltz's timeless truths about competition, conflict, and balancing in a system of structural anarchy no longer rang true. The East-West rivalry was over, arms control agreements seemed to proliferate faster than armaments, democracy spread internationally, and human rights and humanitarian intervention were given practical and not just rhetorical emphasis by many sovereign nation-states [...]"

Foi dentro deste espírito otimista para as relações entre as nações que a Era da Informação começou a se popularizar e consolidar como um caminho sem volta para a grande sociedade mundial. A dependência das novas tecnologias eletrônicas e da comunicação rápida em rede para a mediação das relações entre as indivíduos, instituições e Estados conheceu um crescimento dramático neste período.

> A era digital, é claro, se consolidou na década de 1990. No início deste período quase ninguém ouvira falar de internet, e nós não utilizávamos 'browsers', mecanismos de busca, telefones celulares, jogos 3D ou computadores portáteis. No final desta mesma década, estes [aparelhos] tinham se tornado lugar comum [...] (ANDERSEN, 2015) [9]

As expectativas de um futuro promissor que embalavam o cenário internacional encontraram mais uma promessa de realização nas possibilidades que as novas tecnologias de comunicação começavam a oferecer ao cidadão comum. Grandes transformações estavam a caminho e iriam alterar completamente a maneira como as pessoas interagiam e o mundo se organizava.

> Com o fim do comunismo no leste europeu e a dissolução da URSS a guerra fria acabou, junto com ela terminou também meio século de bipolaridade no sistema internacional [...]
>
> E enquanto os Estados comunistas se desintegravam por si mesmos, uma outra revolução estava ganhando força. Esta revolução silenciosa, ainda na sua infância, é científica e tecnológica. Os seus impactos já foram sentidos e ela promete mudar os hábitos humanos e o sistema internacional tão intensamente, e talvez até mais, do que o colapso do sistema bipolar internacional [...] (ALBERTS; PAPP, 1997, p. 2) [10]

Como resultado das expectativas otimistas projetadas sobre estas tecnologias nascentes, as primeiras visões sobre o que seria ou poderia se tornar o Ciberespaço foram bastante idealistas no sentido de acreditarem que o novo ambiente serviria para promover um nível de desenvolvimento e entendimento humano não visto até então na história humana. O fácil acesso à informação e ao conhecimento humano acumulado, além da sua rápida disseminação pelo planeta, seriam catalizadores de

9 tradução nossa, do original: "THE digital age, of course, got fully underway in the ’90s. At the beginning of the decade almost none of us had heard of the web, and we didn’t have browsers, search engines, digital cellphone networks, fully 3-D games or affordable and powerful laptops. By the end of the decade we had them all [...]"

10 tradução nossa, do original: "With the fall of communism in Eastern Europe and the dissolution of the Soviet Union, the Cold War ended, and the half-century-old bipolar international system disappeared [...]

Even as communist states disintegrated from within, another revolution was accelerating. This quieter revolution, still in its infancy, is a scientific and technological one. It’s impact has already been felt, and it promises to change human affairs and the international system as extensively as, perhaps even more extensively than, the collapse of the bipolar international system [...]"

transformações que iriam criar um mundo melhor para todos.

Tal qual os idealistas de Relações Internacionais, os primeiros usuários da internet acreditavam que a comunicação honesta, sem barreiras ou coerções, disponível para todos os habitantes do planeta, asseguraria o bom entendimento entre as pessoas, grupos e países. A internet seria o meio de se viabilizar este tipo de comunicação através da possibilidade de interligar os pontos mais distantes do planeta e dos novos recursos para troca de informações que ela oferecia. Segundo um dos seus criadores, o cientista da computação Tim Berners-Lee, a possibilidade que os novos documentos de texto digitais ofereciam para acessarem diretamente uns aos outros (conexões de hipertexto que, ao serem clicadas, exibem outros documentos diferentes relacionados) garantiria um novo tipo de organização da informação capaz de revolucionar a maneira como as pessoas trabalhavam.

> Nós vimos que a internet foi inicialmente pensada como um espaço dentro do qual as pessoas pudessem **trabalhar para compartilhar o seu conhecimento**. Isto foi visto como uma poderosa ferramenta porque:
>
> ● quando as pessoas se juntam para construir e compartilhar um [documento de] hipertexto contendo as suas ideias, ele continuará disponível para referência posterior [na internet] a qualquer momento, evitando assim os desentendimentos associados às mensagens lidas uma única vez.
>
> ● quando novas pessoas entram num grupo de trabalho elas encontram fácil acesso [na internet] a todas as decisões e até mesmo aos motivos que têm orientado a condução daquele projeto
>
> ● quando uma pessoa deixa um grupo de trabalho toda a documentação que ela gerou já está armazenada e integrada [ao grupo de documentos principal], nenhum trabalho extra é necessário.
>
> ● com todos os documentos relativos a um dado projeto armazenados na internet, uma análise computacional [via programas específicos] do funcionamento da empresa se torna bastante convidativa permitindo, talvez, tirar conclusões sobre o gerenciamento e reorganização de atividades que um indivíduo teria grandes dificuldades de obter sozinho.
>
> A intenção é que a internet seja utilizada como um sistema pessoal de informação, como uma ferramenta de grupo em todas as escalas a partir de um equipe de dois, como um meio de possibilitar que **a população mundial decida sobre os temas ecológicos** [...] (BERNERS-LEE, 1996, grifo nosso) [11]

11 tradução nossa, do original: "We have seen that the Web initially was designed to be a space within which people could work on an expression of their shared knowledge. This was seen as being a powerful tool, in that

. when people combine to build a hypertext of their shared understanding, they have it at all times to refer to, to allay misunderstandings of one-time messages.
. when new people join a team, they have all the legacy of decisions and hopefully reasons available for their inspection;
. when people leave a team, their work is captured and integrated already, a "debriefing" not being necessary;
. with all the workings of a project on the web, machine analysis of the organization becomes very enticing, perhaps allowing us to draw conclusions about management and reorganization which an individual person would find hard to elucidate;

The intention was that the Web should be used as a personal information system, as a group tool at all scales from the team of two, to the world population deciding on ecological issues [...]"

Um dos ativistas que teve grande impacto neste primeiro momento da internet e do Ciberespaço em geral foi Aaron Swartz. Considerado um gênio precoce ele atuou, ainda na adolescência, em vários projetos voltados para a difusão do conhecimento na internet como a 'Wikipédia' (enciclopédia digital gratuita) e o 'Internet Archive' (tipo de biblioteca digital contendo obras de livre acesso), além de ter ajudado a criar o 'Creative Commons', uma nova proposta de legislação para a propriedade intelectual que incentiva o compartilhamento de ideias e seu aperfeiçoamento em grupo via internet. (KNIGHT, 2013) E se o trabalho técnico de Swartz foi significativo para auxiliar o surgimento de uma cultura cibernética voltada para o bem comum, sua importância como um inspirador e instigador foi ainda maior.

> [...] foi no papel de provocador digital que seu brilhantismo se mostrou com maior intensidade. Trabalhando nos padrões técnicos para o 'Creative Commons' ele ajudou a estender os limites legais que embasavam o software livre para outros empreendimentos criativos, e este impacto foi sentido por toda a internet, ajudando a redefinir a compreensão pública dos direitos de propriedade digital de uma maneira mais ampla (KNIGHT, 2013) [12]

A base do pensamento de Swartz era o "livre acesso", ou seja, enxergar a internet como uma ferramenta para a livre troca de informações de forma que as pessoas fossem capazes de acessar qualquer tipo de conteúdo intelectual, apoderando-se do conhecimento científico pertencente à humanidade visando utilizá-lo em benefício da sociedade e não das grandes corporações.

> Informação é poder, mas como todo poder, há aqueles que querem se apropriar dele. A herança científica e cultural do mundo, publicada através dos séculos em livros e jornais, está sendo digitalizada e tornada inacessível por um pequeno grupo de empresas privadas. Gostaria de ler os artigos descrevendo as mais famosas descobertas da ciência ? Você terá que pagar enormes quantias a editoras como a Reed Elsevier.
>
> [...]
>
> As grandes corporações, é claro, estão cegas pela ganância. As leis sob as quais elas funcionam exigem isso - seus investidores se revoltariam com qualquer coisa diferente. E o mesmo se aplica aos políticos que foram comprados para protegê-las, aprovando leis que as dão poder exclusivo para decidir quem pode fazer cópias.
>
> Não há justiça em seguir leis injustas. Este é o momento de sair à luz e, em nome da grande tradição da desobediência civil, declarar o nosso repúdio a este roubo privado do conhecimento da humanidade.
>
> [...]

12 tradução nossa, do original: "[...] it was in his role as a digital provocateur that his brilliance shone most brightly. By working on the technical standards for the Creative Commons, he helped extend the legal framework behind the free software movement to other creative endeavors. The impact is felt across the Internet and has helped reshape the public's understanding of digital property rights more generally."

> Se houver uma quantidade suficiente de apoio [a esta causa] ao redor do mundo, nós conseguiremos enviar uma forte mensagem contra a privatização do conhecimento e a transformaremos numa coisa do passado. Quer se juntar a nós ? (SWARTZ, 2008) [13]

Entretanto, semelhante ao que aconteceu com as Relações Internacionais no início do século XX, a visão idealista do Ciberespaço não demorou a encontrar forte oposição no desenvolvimento histórico dos fatos. O rápido crescimento no uso da internet para fins comerciais gerou a necessidade de se criar várias medidas de segurança e restrição de acesso, ao invés de incentivos e garantias à liberdade conforme desejavam os seus precursores. Além disso, funcionando como um grande difusor de 'vírus de computadores' (programas que agem de maneira oculta visando prejudicar ou se aproveitar dos usuários de computador), a internet começou a trazer sérios problemas para as pessoas (roubo de dados, perda de informações confidenciais, etc). No alvorecer do século XXI o futuro do Ciberespaço não se mostrava tão alvissareiro quanto imaginaram os seus criadores.

> [...] prevê-se que a movimentação financeira via internet alcance a marca de U$$ 1 trilhão ao fim do ano de 2002. Ninguém pode se dar ao luxo de ignorar a presença do mercado digital e o seu crescimento exponencial. [Por outro lado,] analistas sugerem que não existe uma maneira de se tornar a internet 100% segura, o que obriga as organizações e governos a implementarem políticas de segurança, tanto em termos de software quanto em procedimentos de uso, de maneira a controlar a invasão não autorizada das redes privadas. Os dados corporativos estão em perigo quando expostos à internet [...] (ADETOKUNBO, 2002) [14]

E também nas relações entre os países o neoidealismo da década de 1990 daria lugar à "luta internacional contra o terror" no início do século XXI, logo após os atentados terroristas de 11 de setembro contra os EUA. Novamente as guerras

13 tradução nossa, do original: "Information is power. But like all power, there are those who want to keep it for themselves. The world's entire scientific and cultural heritage, published over centuries in books and journals, is increasingly being digitized and locked up by a handful of private corporations. Want to read the papers featuring the most famous results of the sciences? You'll need to send enormous amounts to publishers like Reed Elsevier.
[...]
Large corporations, of course, are blinded by greed. The laws under which they operate require it — their shareholders would revolt at anything less. And the politicians they have bought off back them, passing laws giving them the exclusive power to decide who can make copies.

There is no justice in following unjust laws. It's time to come into the light and, in the grand tradition of civil disobedience, declare our opposition to this private theft of public culture.
[...]
With enough of us, around the world, we'll not just send a strong message opposing the privatization of knowledge — we'll make it a thing of the past. Will you join us ?"

14 tradução nossa, do original: "[...] predicts that the "Internet economy will top US $1 trillion by the end of 2002." No one can afford to ignore the presence of the Internet economy or its future potential growth. Analysts suggest that there is no way of making the Internet "100 percent safe," therefore, organisations and government are forced to implement security policies, technological software and regulations in order to control unauthorised intrusion into corporate networks [2]. Corporate data are at risk when they are exposed to the Internet [...]"

e os conflitos assumiriam o centro das atenções. Só que desta vez a internet teria um papel preponderante como mediadora na relação do grande público com as notícias aterradoras que rapidamente tomavam conta dos noticiários.

> Os eventos mais cataclísmicos da era da internet foram os atentados de 11 de setembro ao 'World Trade Center', ao Pentágono e a queda do voo 93 da 'United Airlines' na Pensilvânia, antes de atingir o seu alvo em Washington. Para dezenas de milhões de cidadãos estadunidenses, a internet se tornou um canal para suas angústias e orações, para comunicações emocionadas através de e-mail e também para a transmissão de informações vitais [à compreensão dos acontecimentos].
>
> Um ano depois, o impacto do 11 de setembro tem sido sentido de diversas maneiras. Primeiro, uma pesquisa realizada em julho pela 'Pew Internet & American Life Project' mostra que mesmo as pessoas que apoiavam o livre acesso e a divulgação de informações na internet agora apoiam as políticas do governo para remoção de informações da grande rede caso estas sejam consideradas úteis aos terroristas [...]
> [...]
> Segundo, a pesquisa do Instituto Pew sobre o uso da internet nos EUA fornece informações sobre como os hábitos dos usuários mudaram após os ataques:
>
> ● 19 milhões de estadunidenses reataram relações após a tragédia enviando e-mails para membros da família, amigos, antigos colegas de trabalho e outros com os quais eles não se relacionavam há anos.
> ● Um grande número de usuários afirmam que estão utilizando o e-mail com maior frequência, buscando informações na rede com maior frequência, visitando mais vezes os sítios eletrônicos do governo, realizando mais doações via internet e procurando informações sobre saúde mental e física mais vezes do que o faziam antes dos ataques.
>
> Terceiro, a pesquisa mostra que cerca de um décimo dos estadunidenses (11 %) sentem que as suas vidas ainda estão longe de voltar ao normal após os ataques de 11 de setembro e, deste grupo, metade usa a internet. Estes cidadãos mais afetados emocionalmente estão mais dispostos do que os outros usuários a concordar com as decisões do governo em impedir ou restringir o acesso a informações através da internet. Eles afirmam também que aumentaram o uso de e-mails por causa dos ataques terroristas."
> (FOX et al, 2002) [15]

15 tradução nossa, do original: "The most cataclysmic events of the Web era were the 9/11-terror assaults on the World Trade Center, the Pentagon, and the crash of United Airlines Flight 93 in Pennsylvania before it could reach its target in Washington. For tens of millions of Americans, the Internet became a channel for anguished and prayerful gatherings, for heartfelt communication through email, and for vital information.

A year later, the impact of 9/11 is being felt in several ways. First, a survey in July by the Pew Internet & American Life Project shows that even people who favor wide disclosure of information online support government policies to remove that information if officials argue it could aid terrorists [...]
[...]
Second, the Pew Internet Project survey provides evidence about how some Internet users have changed their online behavior in the year since the 9/11 attacks.
● 19 million Americans rekindled relationships after 9/11 by sending email to family members, friends, former colleagues and others that they had not contacted in years. Fully 83% of those who renewed contact with others have maintained those relationships through the past year.
● Notable numbers of American Internet users say they are using email more often, gathering news online more often, visiting government Web sites more often, giving more donations via the Internet, and seeking health and mental health information more often because of the 9/11 attacks.

Third, the survey shows that about a tenth of Americans (11%) feel their lives are still far from normal since the 9/11 events – and of that group, half use the Internet. These hard-hit Americans are more willing than other Internet users to agree with government decisions to remove or withhold information from the Internet. They are also more likely to say they have increased their use of email because of the terror attacks."

Seja como ferramenta de manipulação de opiniões, como um instrumento de esclarecimento, informação ou até de amparo emocional, o Ciberespaço estava consolidado como parte inalienável da vida moderna.

b) Realismo

Esta corrente teórica começou a ganhar força durante a década de 1930 e se manteve em evidência nas décadas seguintes, durante o pós-guerra e toda a Guerra Fria, devido à incapacidade do idealismo liberal em prever e evitar a ascensão do fascismo na Europa, a eclosão da segunda guerra mundial e o conflito ideológico na Guerra Fria (JACKSON; SORENSEN, 2013, p. 39). Os ideais de cooperação e interdependência defendidos pelos liberais não encontraram mais ressonância nos fatos históricos quando as políticas totalitárias, expansionistas e belicosas tomaram conta do cenário internacional

> A mais abrangente e contundente crítica ao idealismo liberal foi feita por E. H. Carr, um acadêmico inglês de Relações Internacionais. No seu livro "A Crise dos Vinte Anos", ele afirma que os pensadores liberais não souberam interpretar os fatos históricos e não entenderam a natureza das relações internacionais. Os liberais acreditavam erroneamente que elas poderiam se basear na harmonia de interesses entre países e nações. Segundo Carr, o ponto de vista correto é o oposto: devemos assumir que existem profundos conflitos de interesse entre países e pessoas [...] (JACKSON; SORENSEN, 2013, p. 39) [16]

Hans J. Morgenthau, outro acadêmico de grande importância para as teorias realistas, afirma em seu livro "A Política entre as Nações" que "[...] a natureza humana é a base das relações internacionais. E os humanos são egoístas e gananciosos, o que pode facilmente levar a agressões [...]" (JACKSON; SORENSEN, 2013, p. 40) [17]

Sob esta perspectiva agora pessimista para com o ser humano, muito influenciada pelos intensos conflitos que marcaram o mundo durante os momentos em que esteve em preponderância, foram definidas três premissas básicas para a teoria realista do sistema internacional (WEBER, 2010, p. 14):

a) A política internacional acontece entre Nações-Estado soberanas.

16 tradução nossa, do original: "The most comprehensive and penetrating critique of liberal idealism was that of E. H. Carr, a British IR scholar. In The Twenty Years' Crisis (1964 [1939]) Carr argued that liberal IR thinkers profoundly misread the facts of history and misunderstood the nature of international relations. They erroneously believed that such relations could be based on a harmony of interest between countries and people. According to Carr, the correct starting point is the opposite one: we should assume that there are profound conflicts of interest both between countries and between people [...]"

17 tradução nossa, do original: "[...] human nature was at the base of international relations. And humans were self-interested and power-seeking and that could easily result in aggression [...]"

b) Não há um governo mundial ou uma autoridade internacional superior capaz de efetivamente impor ordem às relações entre os Estados.

c) A política internacional é anárquica, ou seja, cada uma das Nações-Estado possui liberdade para agir como quiser.

A ausência de uma força superior coercitiva capaz de controlar as relações internacionais leva a uma situação contínua de conflito iminente, fazendo com que as nações estejam sempre se armando e dispostas a guerrear visando assegurar a sua própria sobrevivência. Afirma Kenneth Waltz, um outro autor de grande importância para o realismo:

> Na anarquia não existe tendência à harmonia [...] Um estado utilizará a força para conquistar os seus objetivos se, após avaliar suas possibilidades de sucesso, considerar que os ganhos possíveis [com a guerra] são mais valiosos do que os prazeres da paz. Devido ao fato de cada Estado ser o juiz último de sua própria causa, qualquer Estado, a qualquer tempo, pode utilizar a força para tentar impor as suas políticas. Por isso, todo Estado deve estar constantemente pronto para contra-atacar, sob a pena de pagar o preço da sua fraqueza. E as limitações para que o conflito [armado] aconteça, sob este ponto de vista, são impostas somente pelas circunstâncias na qual cada Estado existe. (WALTZ, 1959, p. 160) [18]

A única maneira de se evitar a guerra na visão realista é o surgimento de uma "balança de poder" onde, no decorrer da escalada armamentista necessária à sobrevivência dos Estados, um determinado Estado tenha sempre um poder bélico equivalente ao poder bélico dos seus rivais, desestimulando, desta forma, a realização de ataques militares contra ele.

> Segundo Waltz esta competição de poder entre os Estados não é tão perigosa quanto pode parecer à primeira vista. Ela não levará necessariamente à guerra desde que um Estado não tenha muito mais poder bélico do que outro Estado ou coalizão de Estados, desde que o conjunto de Estados se mantenha num 'equilíbrio de poder' estável. (WEBER, 2010, p. 22) [19]

O desenvolvimento da compreensão sobre o que é o Ciberespaço no início do século XXI, logo após o início da "guerra ao terror", sofreu uma grande influência da

18 tradução nossa, do original: "In anarchy there is no automatic harmony [...] A state will use force to attain its goals if, after assessing the prospects for success, it values those goals more than it values the pleasures of peace. Because each state is the final judge of its own cause, any state may at any time use force to implement its policies. Because any state may at any time use force, all states must constantly be ready either to counter force with force or to pay the cost of weakness. The requirements of state action are, in this view, imposed by the circumstances in which all states exist."

19 tradução nossa, do original: "[...] According to Waltz, this competition for power among states is not always as dangerous as it at first sounds. It doesn't have to lead to war, so long as no state has significantly more power than another state or coalition of states, so long as states in combination are in a stable 'balance of power' arrangement."

perspectiva belicista e militar que projetou sobre o meio virtual a visão de um novo espaço operacional, um domínio independente e peculiar de ação diferente dos outros já existentes (terra, mar, ar e espaço sideral) (KUEHL, 2009, p. 1-4)

Entre os diversos autores que estudam o Ciberespaço e adotaram esta linha de pensamento em maior ou menor grau, Richard Clarke e Robert Knake são exemplos da abordagem realista. Sobre os atores envolvidos nos conflitos cibernéticos, eles afirmam que a guerra cibernética "[...] se refere a ações perpetradas por Nações-Estado sobre computadores ou redes de outras Nações-Estado com o propósito de causar danos ou interrupção [de serviço] [...]" (CLARKE; KNAKE, 2010, p. 6) [20]. Deixando bem clara, desta forma, a visão estadocêntrica do fenômeno e a percepção da soberania como elemento fundamental à análise desenvolvida. Mais ainda, no entender destes autores, a guerra cibernética é iminente, ubíqua e terá consequências devastadoras para as nações que não estiverem preparadas para ela. Eles resumem a situação atual em cinco sentenças básicas:

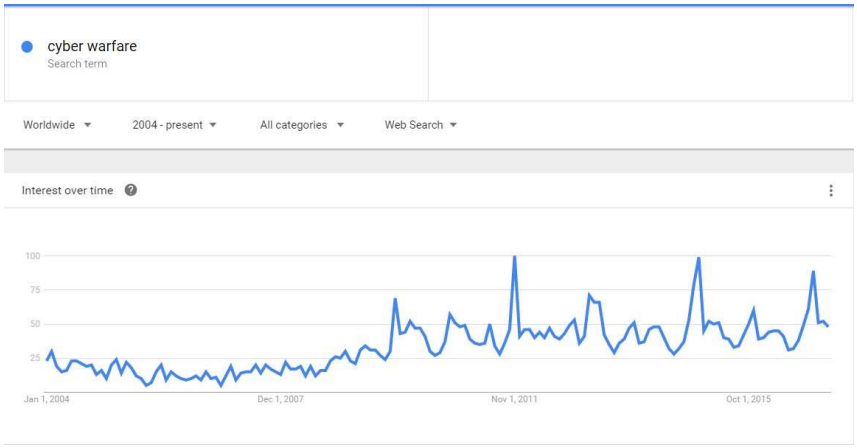
> **A guerra cibernética é real**: o que nós temos visto até o momento está longe de demonstrar o que [os Estados] realmente são capazes. A maioria dos conflitos [que têm acontecido] utilizam apenas armas cibernéticas primitivas (com a notável exceção da operação israelense). Trata-se de uma suposição razoável afirmar que os atacantes não têm interesse em revelar os seus recursos mais sofisticados neste [primeiro] momento. O que os EUA e algumas outras Nações são capazes de fazer numa guerra cibernética pode devastar um país.
> **A guerra cibernética acontece na velocidade da luz**: o intervalo de tempo que os fótons do pacote de dados atacante levam para chegar até a sua vítima, trafegando pela rede digital [internacional] de fibras óticas, é [ínfimo e] praticamente imperceptível, gerando assim uma grande possibilidade de crise para os responsáveis pelas decisões cabíveis [incapacidade de reagir a tempo].
> **A guerra cibernética é global**: em qualquer conflito [cibernético] os ciberataques rapidamente se tornam mundiais na medida em que [vários] outros computadores pessoais e servidores [espalhados pela rede e] cooptados [à revelia dos seus usuários] pelos 'hackers' participam do ataque. Muitas nações tomam parte do assalto [sem se dar conta disto].
> **A guerra cibernética se expande para fora do campo de batalha**: os sistemas dos quais as pessoas dependem [para agir dentro da sociedade atual], desde bancos até sistemas de radar, são acessíveis através do ciberespaço e podem ser rapidamente controlados ou desligados sem que, para isso, seja necessário enfrentar o sistema militar de defesa do país.
> **A guerra cibernética já começou**: na tentativa de antecipar as hostilidades as nações estão preparando o 'campo de batalha'. Elas estão espionando as redes e sistemas de infraestrutura [dos outros países], e implantando armadilhas e bombas lógicas agora, em tempos de paz. Esta natureza contínua da guerra cibernética, confundindo guerra e paz, acrescenta uma perigosa nova dimensão de instabilidade [à sociedade].
> (CLARKE ; KNAKE, 2010, pp. 30-31) [21]

20 tradução nossa, do original: "[...] 'cyber war' [...] refers to actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption [...]".

Podemos observar que as premissas básicas da visão realista se encontram claramente embutidas nestas afirmações que embasam o trabalho dos autores: a iminência do conflito e a urgência da necessidade de preparação ("a guerra cibernética já começou"), a abrangência global do fenômeno num sistema anárquico onde nenhum Estado possui controle total do ciberespaço ("a guerra cibernética é global e se expande para fora do campo de batalha"), além da percepção de que o desenvolvimento da capacidade bélica cibernética é essencial para a sobrevivência dos Estados ("a guerra cibernética é real e acontece na velocidade da luz").

A ideia de 'Guerra Cibernética' começou a ganhar popularidade ao longo da primeira década do século XXI, conforme sugerem as estatísticas de busca pelo termo 'cyber warfare' (Guerra Cibernética) fornecidas pelo 'Google Trends' (ferramenta que permite consultar percentualmente e ao longo do tempo a quantidade de entradas para um determinado termo no sítio de buscas da empresa 'Google').

Figura 2 - buscas realizadas no período de 2004 a 2017 para
o termo 'cyber warfare' na ferramenta de pesquisa da empresa 'Google'.



Fonte: 'Google Trends'

21 tradução nossa, do original:
"Cyber war is real. What we have seen so far is far from indicative of what can be done. Most of these well-known skirmishes in cyberspace used only primitive cyber weapons (with the notable exception of the Israeli operation). It is a reasonable guess that the attackers did not want to reveal their more sophisticated capabilities, yet. What the United States and other nations are capable of doing in a cyber war could devastate a modern nation.
Cyber war happens at the speed of light. As the photons of the attack packets stream down fiber-optic cable, the time between the launch of an attack and its effect is barely measurable, thus creating risks for crisis decision makers.
Cyber war is global. In any conflict, cyber attacks rapidly go global, as covertly acquired or hacked computers and servers throughout the world are kicked into service. Many nations are quickly drawn in.
Cyber war skips the battlefield. Systems that people rely upon, from banks to air defense radars, are accessible from cyberspace and can be quickly taken over or knocked out without first defeating a country's traditional defenses.
Cyber war has begun. In anticipation of hostilities, nations are already "preparing the battlefield." They are hacking into each other's networks and infrastructures, laying in trapdoors and logic bombs—now, in peacetime. This ongoing nature of cyber war, the blurring of peace and war, adds a dangerous new dimension of instability."

Figura 2: Disponível em <https://trends.google.com/trends/explore?date=all&q=cyber%20warfare> Acesso em 29 fev 2017.

Vários incidentes importantes envolvendo o Ciberespaço e ocorridos durante a década de 2000 receberam ampla cobertura jornalística internacional, incentivando o interesse popular na ideia de um conflito digital de grandes proporções, entre eles: os ataques cibernéticos realizados pelos EUA contra o Irã utilizando o vírus chamado 'stuxnet' que vieram a público em 2008 (vide capítulo 4), a sabotagem dos serviços de internet na Geórgia visando facilitar a intervenção militar russa em 2007 (vide capítulo 3), os ataques da China contra a empresa Google nos EUA em 2009 e vários outros. A percepção de que as sociedades modernas haviam se tornado muito dependentes da internet e que esta rede mundial poderia ser utilizada para viabilizar ataques militares ou enfraquecer a capacidade de reação dos países diante dos seus possíveis inimigos gerou uma sensação de 'catástrofe iminente' no imaginário popular onde até mesmo os apagões ocorridos no Brasil em 1998 passaram a ser vistos como possíveis consequências de ataques cibernéticos. Um artigo de jornal desta época apresentado a opinião de um especialista é um exemplo deste tipo de avaliação.

> A ameaça de guerra cibernética tem sido muito exagerada, afirma um conceituado especialista em segurança digital. Bruce Schneier explica que a retórica emotiva em torno do termo não corresponde à realidade e adverte que o uso de termos como 'armagedon digital' aumenta ainda mais o equívoco [...] Ele sugere que este exagero tenha surgido devido aos vários incidentes de grande repercussão ocorridos nos últimos anos, incluindo os apagões na rede elétrica do Brasil, ataques da China contra a Google e o vírus stuxnet utilizado para tentar destruir as instalações nucleares iranianas. Além disso, as revelações divulgadas pelo site Wikileaks e o roubo dos e-mails da candidata rebublicana à vice-presidência, Sarah Palin, também têm incentivado este tipo de reação. Afirma Schneier: "O que nós temos visto não é uma guerra cibernética mas o aumento do uso de táticas de guerra [no ciberespaço], e isto é o que tem causado confusão. Nós não temos uma boa definição para o que é guerra cibernética, como ela acontece ou quais armas ela efetivamente utiliza." Falando para um pequeno grupo de repórteres ele continua: "guerra cibernética é uma metáfora que não abrange os problemas que estamos abordando, são eles: ciberespionagem, crimes cibernéticos, roubo de identidades, fraudes de cartões de crédito, etc. Não transformem o termo em algo que ele não é." (SHIELS, 2011) [22]

22 tradução nossa, do original: "The threat of cyber warfare is greatly exaggerated, according to a leading security expert. Bruce Schneier claims that emotive rhetoric around the term does not match the reality. He warned that using sensational phrases such as "cyber armageddon" only inflames the situation [...] He suggested that the notion of a cyber war was based on several high-profile incidents from recent years. They include blackouts in Brazil in 1998, attacks by China on Google in 2009 and the Stuxnet virus that attacked Iran's nuclear facilities. He also pointed to the fallout from Wikileaks and the hacking of Republican vice-presidential candidate Sarah Palin's e-mail. "What we are seeing is not cyber war but an increasing use of war-like tactics and that is what is confusing us. We don't have good definitions of what cyber war is, what it looks like and how to fight it," said Mr Schneier. "Cyber war is a turbo metaphor that does not address the issues we are looking at like cyber espionage, cyber crime, identity theft, credit card fraud. When you look at the conflict environment - military to military - command and control is always part of the thing. Don't make it something that it is not," Mr Schmidt told a small group of reporters [...]"

A falta de consenso sobre o que realmente seria uma 'guerra cibernética', a clara percepção de que há muitos atores e interesses atuando diretamente na internet além dos Estados, e a dependência cada vez maior das sociedades modernas, nos mais diversos tipos de atividades, para com os sistemas digitais de comunicação, estimularam outros tipos de análises sobre as possibilidades de poder no Ciberespaço que iriam além da perspectiva militar e estadocêntrica realista.

c) Neoliberalismo

Os anos após a Segunda Guerra Mundial e durante a Guerra Fria foram marcados pela disputa de poder e a expectativa de conflito iminente entre os EUA e a URSS, o que influenciou fortemente os estudos de relações internacionais na direção da visão realista de mundo. Entretanto, ao mesmo tempo em que a interação entre as nações nesta época era delimitada pela bipolaridade, o esforço de reconstrução da Europa e o incentivo ao desenvolvimento dos países mais pobres do bloco ocidental (política externa dos EUA na época visando evitar que o lado comunista ganhasse mais adeptos) geraram um forte estímulo ao comércio internacional que foi se tornando cada vez mais intenso nas regiões do mundo sob influência estadunidense (MILANI, 2014, p. 35). Desta forma, laços pacíficos de relações não só comerciais mas também culturais e humanas em diversos níveis foram surgindo entre os países, levando gradualmente à percepção de que uma realidade distinta do paradigma bélico realista estava em curso. Para os liberais, pelo menos até certo ponto, isto representava um ressurgimento das suas ideias e valores.

> Durante as décadas de 1950, 1960 e 1970 uma boa parte das relações internacionais estavam direcionadas para comércio e investimentos, viagens e comunicação, além de outros temas similares que adquiriram primazia nas interações entre as democracias liberais ocidentais. Essas relações ofereceram o ponto de partida para uma nova tentativa dos liberais em formular uma maneira de pensar o mundo que representasse uma alternativa aos realistas e, ao mesmo tempo, evitasse as excessivas utopias do Idealismo. Utilizaremos o termo 'neoliberalismo' para identificar esta nova abordagem [...] (JACKSON; SORENSEN, 2013, p. 46) [23]

Mas para que os liberais conseguissem reformular de maneira convincente

23 tradução nossa, do original: "[...] during the 1950s, 1960s, and 1970s, a good deal of international relations concerned trade and investment, travel and communication, and similar issues which were especially prevalent in the relations between the liberal democracies of the West. Those relations provided the basis for a new attempt by liberals to formulate an alternative to realist thinking that would avoid the utopian excesses of earlier liberalism. We shall use the label ‘neoliberalism’ for that renewed liberal approach [...]"

suas ideias anteriormente consideradas utópicas era necessário buscar bases mais sólidas e que estivessem de acordo com o pensamento científico predominante. Foi neste sentido que a metodologia behaviorista, muito valorizada nos EUA após a Segunda Guerra Mundial por defender o uso de métodos quantitativos (busca por padrões estatísticos que permitam gerar classificações e generalizações para os fenômenos internacionais), passou a ser utilizada para embasar a construção das teorias neoliberais de relações internacionais, abandonando a metodologia humanista anterior (estudos filosóficos baseados em Direito e História).

> [...] os neoliberais compartilham as velhas ideias liberais sobre as possibilidades de progresso e mudança, mas repudiam o idealismo. Eles também se esforçam por formular teorias e utilizar métodos que são científicos. Para resumir, o debate entre liberalismo e realismo [em relações internacionais] continuou, mas ele agora assumiu novos tons devido ao contexto da Guerra Fria e a persuasão metodológica behaviorista (JACKSON; SORENSEN, 2013, p. 46) [24]

O sistema internacional ocidental durante o período da Guerra Fria teve como centro o poderio militar e comercial dos EUA que, enxergando o comércio internacional como uma barreira contra o expansionismo territorial e ideológico da URSS, estimulou a intensificação dos laços comerciais entre as nações aliadas (MILANI, 2014, p. 35). Neste espaço geopolítico, muitas das relações entre os países tendiam a acontecer de maneira pacífica e diversificada.

> [...] Durante as décadas de 1950 e 1960 a Europa Ocidental e o Japão desenvolveram mercados de consumo de massa apoiados em políticas de bem-estar social ['welfare state'] semelhantes às que os EUA já haviam implementado antes da Segunda Guerra Mundial. Este modelo de desenvolvimento possibilitou uma alta interatividade em termos de comércio, comunicação, trocas culturais e outros tipos de relações além-fronteiras.
>
> A percepção desta realidade forneceu a base para o liberalismo social, uma vertente do pensamento neoliberal que valoriza o impacto destas interações mais intensas entre os países. Em 1950, Karl Deutsch e outros enfatizaram que as interconexões ajudavam a criar valores e identidades comuns entre as pessoas de diferentes países e [, desta forma,] pavimentaram o caminho para relações de cooperação pacíficas, tornando assim a guerra cada vez mais custosa para as partes envolvidas e, por isso, cada vez mais improvável. (JACKSON; SORENSEN, 2013, p. 47) [25]

24 tradução nossa, do original: "[...] Neoliberals share old liberal ideas about the possibility of progress and change, but they repudiate idealism. They also strive to formulate theories and apply new methods which are scientific. In short, the debate between liberalism and realism continued, but it was now coloured by the post-1945 international setting and the behaviouralist methodological persuasion."

25 tradução nossa, do original: "[...] During the 1950s and 1960s, Western Europe and Japan developed mass-consumption welfare states, as the United States had done already before the war. That development entailed a higher level of trade, communication, cultural exchange, and other relations and transactions across borders.
This provides the basis for sociological liberalism, a strand of neoliberal thinking which emphasizes the impact of these expanding cross-border activities. In the 1950s, Karl Deutsch and his associates argued that such interconnecting activities helped create common values and identities among people from different states and paved the way for peaceful, cooperative relations by making war increasingly costly and thus more unlikely."

Na visão do liberalismo social o contato entre os países transborda das relações comerciais para as relações humanas em geral fazendo com que a interdependência comercial, na prática, acabe se ampliando para várias áreas das atividades humanas, gerando o que passou a se chamar 'interdependência complexa'. Uma perspectiva que faz com que o poderio militar deixe de ser preponderante para as relações internacionais.

> Foi na década de 1970 que Robert Keohane e Joseph Nye desenvolveram estas ideias. Eles argumentavam que as relações entre os Estados ocidentais (incluindo o Japão) eram caracterizadas pela interdependência complexa: há muitas formas [diferentes] de contato entre as sociedades além da relações políticas entre os governos, incluíndo aí as conexões criadas pelas empresas transnacionais. Também, não há uma 'hierarquia entre temas', ou seja, a segurança militar não mais domina as conversações entre os países. A força militar não é mais utilizada como um instrumento de política externa (JACKSON; SORENSEN, 2013, p. 47) [26]

A 'Interdependência Complexa' transfere o foco das relações internacionais para fora do âmbito militar e para dentro das interações humanas, colocando assim uma perspectiva otimista, pacífica e bastante diversificada para o Sistema Internacional.

> A Interdependência Complexa enxerga uma situação que é radicalmente diferente da imagem projetada pelos realistas para as relações internacionais. Para as democracias ocidentais há outros atores além dos Estados e os conflitos violentos claramente não interessam a eles. Este tipo de visão neoliberal é chamada liberalismo de interdependência. Robert Keohane e Joseph Nye estão entre as principais influências desta linha de pensamento (JACKSON; SORENSEN, 2013, p. 47) [27]

O fim da Guerra Fria no início da década de 1990 e a aparente primazia do liberalismo econômico sobre as suas ideologias antagonistas trouxe, além do otimismo neoliberal, novas perspectivas para um modelo econômico e político em franca expansão. A interdependência complexa, agora envolvendo todas as nações do planeta, consolidaria a democracia liberal como o único sistema de governo das nações num mundo sob hegemonia dos EUA. O teórico Francis Fukuyama, grande defensor deste tipo de interpretação para os acontecimentos históricos em

26 tradução nossa, do original: "In the 1970s, Robert Keohane and Joseph Nye further developed such ideas. They argued that relationships between Western states (including Japan) are characterized by complex interdependence: there are many forms of connections between societies in addition to the political relations of governments, including transnational links between business corporations. There is also an ‘absence of hierarchy among issues’, i.e., military security does not dominate the agenda any more. Military force is no longer used as an instrument of foreign policy [...]"

27 tradução nossa, do original: "[...] Complex interdependence portrays a situation that is radically different from the realist picture of international relations. In Western democracies, there are other actors besides states, and violent conflict clearly is not on their international agenda. We can call this form of neoliberalism interdependence liberalism. Robert Keohane and Joseph Nye (1977) are among the main contributors to this line of thinking."

andamento nesta época, chegou a afirmar que a humanidade havia alcançado o "fim da história". Segundo ele, a história das ideias políticas humanas havia terminado. A democracia liberal vencera a batalha das ideologias e, daí pra frente, restava-lhe somente se expandir e conquistar todo o planeta. A percepção de que não havia mais adversários para a economia liberal aliada às ideias de Fukuyama sobre a sua inevitável prevalência histórica geraram grandes discussões sobre os possíveis impactos e consequências de uma estrutura econômica e política mundial única, um fenômeno que passou a ser chamado de 'globalização'.

> Fukuyama argumenta que a democracia liberal como um sistema de governança conquistou uma 'vitória absoluta' sobre os outros sistemas de ideias de maneira que o liberalismo é a única ideologia legítima que restou no mundo. Não só deixaram de existir adversários ideológicos para o liberalismo como o liberalismo, ele mesmo, é livre de contradições internas, causando o colapso dos seus oponentes. Não possuir contradições internas significa que o liberalismo é uma ideia acabada [não admite melhorias ou revisões]. E para Fukuyama isto marca o 'ponto final da evolução ideológica humana' e significa que o liberalismo é a 'forma final de governo humano' [...] A crença de Fukuyama não só previu o término do paradigma estratégico da guerra fria como permitiu também o surgimento de um campo totalmente novo de estudos: a globalização."
> (WEBER, 2010, p. 108) [28]

O fenômeno da globalização recebeu uma enorme atenção acadêmica na virada para o século XXI, com muitos autores desenvolvendo estudos sobre os mais variados aspectos deste tema. Entretanto, a grande diversidade de abordagens e a falta de um consenso sobre o que efetivamente seria a globalização impossibilitou a elaboração de uma definição mais ampla e, desta forma, terminou por invalidar o uso do termo.

> A globalização se tornou o tema da moda em teoria de Relações Internacionais na virada do século mas ... O que é globalização ? Trata-se de uma boa pergunta que os acadêmicos dentro e de fora do campo das Relações Internacionais têm grande dificuldade em responder. A globalização tem sido descrita como 'um termo que pode se referir a qualquer coisa entre internet e hamburguer'. E isso acontece porque os teóricos discordam em quase tudo relacionado com a globalização [...]
> (WEBER, 2010, p. 108) [29]

28 tradução nossa, do original: "Fukuyama argues that liberal democracy as a system of governance has won an "unabashed victory" over other ideas to the point that liberalism is the only legitimate ideology left in the world. Not only are there no coherent ideological challengers to liberalism, liberalism itself is free of irrational internal contradictions which lead to the collapse of ideologies. Having no internal contradictions means that liberalism is a finished idea. For Fukuyama, all this marks "the end point of mankind's ideological evolution" and means that liberalism is "the final form of human government' [...] Fukuyama's myth not only foretold the death of the classical Cold War strategic paradigm, it made possible an entirely new realm of research—the study of 'globalization'. "

29 tradução nossa, do original: "Globalization became the trendiest craze in IR theory at the turn of the century. What is globalization ? That's a good question, and one with which scholars in and out of IR have had difficulty grappling. Globalization has been described as 'a term which can refer to anything from the Internet to a hamburger'. That's because theorists disagree on just about everything regarding 'globalization.' "

Mas esta falta de definição não impediu que, dentro da visão neoliberal, a globalização passasse a ser vista como a realização mundial dos grandes ideais do liberalismo social: um sistema internacional unificado estava surgindo e iria levar o mundo para um novo patamar de estabilidade e grandes realizações através da interação cada vez mais harmoniosa entre os povos.

> Na era da 'globalização' os princípios liberais clássicos se tornaram interpretações neoliberais para este fenômeno. Nele, três processos acontecem simultaneamente para o bem da humanidade: liberalismo econômico (livre comércio), democratização (poder para o povo) e universalização da cultura (que alguns chamariam de 'americanização global'). Para os neoliberais, globalização é a propagação benéfica dos valores liberais em termos de economia, política, cultura, instituições e práticas por todo o mundo. (WEBER, 2010, p. 109) [30]

E dentro desta perspectiva de melhoria constante das sociedades o princípio liberal de maior importância é a crença no progresso através do desenvolvimento tecnológico, uma benesse que a interdependência complexa espalharia por todo o planeta durante o século que se iniciava. Para os neoliberais a ação racional através da tecnologia garante que o ser humano será capaz de produzir cada vez mais e melhor, gerando vantagens para uma quantidade crescente de pessoas.

> O processo de modernização deflagrado pela revolução científica levou a tecnologias cada vez melhores e, desta forma, a meios cada vez mais eficientes para a produção de bens e domínio da natureza. Esta visão benfazeja da tecnologia foi reforçada pela revolução intelectual liberal que tinha grande fé na razão humana e na racionalidade. Esta é a base para a crença liberal no progresso: o Estado liberal moderno produz um sistema político e econômico que traz, nas palavras de Jeremy Benthan, a 'maior felicidade para o maior número de pessoas'. (JACKSON; SORENSEN, 2013, p. 100) [31]

No início do século XXI o aspecto mais vísivel do progresso tecnológico é também a parte mais conhecida do Ciberespaço, a internet, uma intermediadora cada vez mais pervasiva da comunicação globalizada e um meio privilegiado de viabilização da interdependência complexa.

30 tradução nossa, do original: "In an era of 'globalization,' classical liberal principles become neoliberal expressions of 'globalization,' in which three processes occur simultaneously and for the good of humankind—economic liberalization (like free trade), political democratization (power to the people), and cultural universalization (some would say the 'Americanization' of the globe). For neoliberals, 'globalization' is about the benevolent spread of liberal economic, political, and cultural processes, institutions, and practices throughout the world."

31 tradução nossa, do original: "The process of modernization unleashed by the scientific revolution led to improved technologies and thus more efficient ways of producing goods and mastering nature. That was reinforced by the liberal intellectual revolution which had great faith in human reason and rationality. Here is the basis for the liberal belief in progress: the modern liberal state invokes a political and economic system that will bring, in Jeremy Bentham's famous phrase, 'the greatest happiness of the greatest number'."

> A dimensão da interdependência complexa que mais se alterou desde a década de 1970 são os canais de contato entre as sociedades. Tem havido uma enorme expansão destes canais, resultado da dramática queda nos custos de comunicação à longa distância. Não mais é necessário ser uma empresa rica para poder se comunicar em tempo real com pessoas ao redor do mundo. Friedman chama esta mudança de 'democratização' da tecnologia, finanças e informação devido ao fato desta redução de custo ter transformado um luxo restrito a poucos num lugar comum acessível à grande parte da sociedade (KEOHANE; NYE JR, 2000, p. 116) [32]

Para Robert Keohane e Joseph Nye Jr, dois grandes nomes do pensamento neoliberal, a transformação que caracteriza o início do século XXI é a velocidade com que as instituições passam a se comunicar, permitindo, desta forma, a intensificação da interdependência complexa através do estreitamento dos laços sociais e culturais. As novas tecnologias de comunicação, particularmente o Ciberespaço e a internet, são os meios por onde esta transformação acontece.

> No final dos anos 70 o ciclo de divulgação das notícias pela imprensa mantinha o mesmo ritmo que o caracterizou por várias décadas: as pessoas tomavam conhecimendo das manchetes do dia assistindo ao noticiário noturno e, na manhã seguinte, liam uma análise mais detalhada e completa das notícias nos jornais impressos matinais. Mas quando a TV a cabo começou a funcionar 24 horas por dia, durante a década de 1980, aliada ao surgimento da internet [nos países desenvolvidos], os ciclos de notícias se tornaram [cada vez] mais curtos e os veículos de comunicação começaram a competir por pequenas vantagens de tempo [ao divulgar os últimos acontecimentos] [...] De tal maneira que quando chegamos na década de 2000 intervalos de uma hora e às vezes poucos minutos já representavam uma diferença decisiva para as TVs em termos de estarem atualizadas ou não com as últimas notícias. E a velocidade institucional cresceu mais rapidamente até do que a velocidade das mensagens. A velocidade institucional reflete não somente conexões entre as instituições mas também a existência de redes e de conexões entre redes. É neste fenômeno que está a grande mudança. (KEOHANE; NYE JR, 2000, p. 114) [33]

Entretanto, o início do século XXI também trouxe acontecimentos de forte impacto político e emocional que comprometeram de maneira definitiva a visão

32 tradução nossa, do original: "The dimension of complex interdependence that has changed the most since the 1970s is participation in channels of contact among societies. There has been a vast expansion of such channels as a result of the dramatic fall in the costs of communication over large distances. It is no longer necessary to be a rich organization to be able to communicate on a real-time basis with people around the globe. Friedman calls this change the "democratization" of technology, finance, and information because diminished costs have made what were once luxuries available to a much broader range of society."

33 tradução nossa, do original: "In the late 1970s, the news cycle was the same as it had been for decades: People found out the day's headlines by watching the evening news and got the more complete story and analysis from the morning paper. But the introduction of 24-hour cable news in 1980 and the subsequent emergence of the Internet have made news cycles shorter and have put a larger premium on small advantages in speed [...] in 2000, an hour - or even a few minutes - makes a critical difference for a cable television network in terms of being "on top of a story" or "behind the curve." Institutional velocity has accelerated more than message velocity. Institutional velocity reflects not only individual linkages but networks and interconnections among networks. This phenomenon is where the real change lies"

otimista neoliberal em ascensão após o fim da Guerra Fria. A destruição das torres gêmeas em Nova Iorque e os ataques a outras cidades dos EUA, junto com os vários atentados terroristas ocorridos na Europa, projetaram uma sombra de instabilidade política sobre o cenário internacional que iria levar à chamada 'Guerra ao Terror' e ao fim das expectativas de uma globalização pacífica e alvissareira.

> [...] houve uma nova onda de otimismo liberal após o fim da Guerra Fria, impulsionada pelas ideias de "fim da história" e oriunda da derrota do comunismo e da expectativa de uma vitória universal da democracia liberal. Entretanto, os ataques terroristas a Nova Iorque e Washington em 11 de setembro, seguidos dos ataques a Madri, Londres e várias outras cidades representaram um revés a este otimismo liberal (JACKSON; SORENSEN, 2013, p. 101) [34]

Estes acontecimentos trágicos reduziram a força dos argumentos neoliberais devido ao foco militarista subitamente assumido no cenário internacional pelos países desenvolvidos, mas não os invalidaram por completo. A ressurgência de perspectivas belicosas em algumas partes do mundo não nega o fato de que, em outras regiões mais afortunadas, a interdependência complexa continuava atuando de maneira benéfica.

> Maior capacidade de interação à distância e maior aproximação [dos países] devido à interdependência complexa não significa o fim da política, pelo contrário: o poder continua sendo importante. Mesmo nos domínios influenciados pela interdependência complexa a política reflete assimetrias em termos econômicos, sociais e ambientais, não somente entre Estados mas também entre atores não estatais e nas relações transnacionais. A interdependência complexa não é uma descrição do mundo mas sim um modelo ideal que representa uma abstração da realidade [conceito Weberiano]. Entretanto, trata-se de um modelo que se aproxima cada vez mais da realidade em muitas partes do mundo, mesmo através de distâncias transcontinentais; um modelo muito mais fidedigno do que aquelas imagens antigas de política internacional como relações estadocêntricas interessadas somente em força militar e segurança. (KEOHANE; NYE JR, 2000, p. 114) [35]

34 tradução nossa, do original: " [...] there was another surge of liberal optimism after the end of the Cold War, propelled by the notion of ‘the end of history’ based on the defeat of communism and the expected universal victory of liberal democracy (Fukuyama 1989, 1992). However, the terrorist attacks in New York and Washington of 11 September 2001, followed by the attacks in Madrid, London, and elsewhere, are a setback for liberal optimism."

35 tradução nossa, do original: "Increased participation at a distance and greater approximation of complex interdependence do not imply the end of politics. On the contrary, power remains important. Even in domains characterized by complex interdependence, politics reflects asymmetrical economic, social, and environmental interdependence, not just among states but also among nonstate actors, and through transgovernmental relations. Complex interdependence is not a description of the world, but rather an ideal concept abstracting from reality. It is, however, an ideal concept that increasingly corresponds to reality in many parts of the world, even at transcontinental distances - and that corresponds more closely than obsolete images of world politics as simply interstate relations that focus solely on force and security."

Na mesma medida em que o Ciberespaço e sua manifestação mais visível, a internet, se consolidaram como um meio de ampliação e expansão dos canais de contato entre as sociedades, reduzindo grandemente os ciclos de divulgação dos acontecimentos, aumentando a velocidade instituicional e criando cada vez mais redes de interconexão ao redor do mundo (numa tradução digital das esperanças de progresso globalizado neoliberal); as grandes assimetrias globais encontraram neste mesmo Ciberespaço um lócus privilegiado para a projeção e exercício dos seus conflitos, seja em termos de explicitação das contradições do sistema (divulgação não controlada de catástrofes econômicas e humanas nos países mais pobres, blogs exibindo propaganda antiliberal, etc), terrorismo (aliciamento de membros, planejamento de operações via redes privadas criptografadas, propaganda ideológica, etc) ou militares (apoio a operações de guerra e ataques físicos contra outros Estados), seja em termos de consolidação dos laços de globalização entre as nações (aceleração do comércio globalizado e da interdependência entre as nações). Diferente de outros contextos, onde o poder financeiro define o mais forte e mais capaz, o Ciberespaço permite que, pelo menos até certo ponto, atores menores e mais fracos consigam significativo poder de ação e influência. Este caráter ambíguo e indefinido do Ciberespaço, possibilitando a refutação e a reafirmação da globalização neoliberal além da efetiva manifestação de atores até então menos expressivos e poderosos, o transforma num meio multifacetado para o exercício de poder em diversos níveis e sob interesses bastante variados.

> O poder depende do contexto e [neste sentido] o rápido crescimento do Ciberespaço é um importante novo contexto no mundo político. O baixo custo de entrada, o anonimato e as assimetrias em vulnerabilidade significam que atores menores têm maior capacidade de exercer [...] poder no Ciberespaço do que em muitos outros domínios tradicionais da política [...] (NYE JR, 2011, p. 1) [36]

Entretanto, independente dos interesses que movimentam os seus muitos e diversificados atores, o Ciberespaço é talvez o principal e mais importante meio para a realização da globalização neoliberal e esta importância é refletida pela enorme velocidade e intensidade da sua expansão.

36 tradução nossa, do original: "Power depends upon context, and the rapid growth of cyber space is an important new context in world politics. The low price of entry, anonymity, and asymmetries in vulnerability means that smaller actors have more capacity to exercise [...] power in cyberspace than in many more traditional domains of world politics [...]"

> Em 1993 havia cerca de 50 páginas eletrônicas (*websites*) no mundo. No final desta mesma década este total já havia passado dos 5 milhões e, em 2010, somente a China tinha cerca de 400 milhões de usuários de internet. A largura de banda de internet [parâmetro que define a quantidade máxima de informação que pode trafegar na rede num dado instante de tempo] está se expandindo rapidamente enquanto os seus custos continuam a cair mais depressa até do que os custos da capacidade de processamento dos computadores. Na década de 1980 ligações telefônicas em cabos de cobre conseguiam transmitir apenas uma página de informação por segundo. Hoje em dia um fio de fibra ótica, com diâmetro diminuto, é capaz de transmitir cerca de 90.000 volumes por segundo. Em 1980 um gigabyte de armazenamento ocupava uma sala inteira, atualmente mais de 200 gigabytes cabem no bolso da sua camisa. A quantidade de informação digital aumenta cerca de 10 vezes a cada 5 anos. O que isto tudo significará em termos de poder e governança no século XXI ? (NYE JR, 2011, p. 2) [37]

Quanto mais rápido o Ciberespaço se expande pelo planeta e invade os interstícios das individualidades modernas, mais a informação (controlada ou não) circula pelas diferentes culturas e sociedades globais, abrindo novos campos de contato, interferência e influência mútua. A interdependência complexa globalizada acontece tanto contra quanto a favor da estrutura política neoliberal, difundindo o poder para espaços até então considerados insignificantes ou inexistentes.

> A transição de poder de um estado de dominação para outro é um evento histórico bem conhecido, mas a difusão de poder é um processo totalmente novo. O grande problema de todos os países nesta Era da Informação global é que mais e mais coisas estão acontecendo fora do círculo de controle até mesmo das nações mais poderosas. Nas palavras de um ex-diretor de planejamento de políticas de Estado: 'a proliferação de informação é tanto a causa da não-polaridade quanto a proliferação de armamentos' (NYE JR, 2011, p. 1) [38]

Dentro desta perspectiva de intensa interconexão e comunicação fácil, rápida e constante entre as sociedades mundiais, a informação se torna então um ativo de grande valor e importância, e a sua manipulação por atores variados dentro do cenário internacional, influênciando simultaneamente milhares ou milhões de

37 tradução nossa, do original: "In 1993, there were about 50 websites in the world; by the end of the decade, that number had surpassed 5 million. By 2010, China alone had nearly 400 million users. Communications bandwidths are expanding rapidly, and communications costs continue to fall even more rapidly than computing power. As recently as 1980, phone calls over copper wire could carry only one page of information per second; today a thin strand of optical fiber can transmit 90,000 volumes in a second. In 1980, a gigabyte of storage occupied a room; now 200 gigabytes of storage fits in your shirt pocket. The amount of digital information increases tenfold every five years. What will this mean for power and governance in the 21st century ?"

38 tradução nossa, do original: "Power transition from one dominant state to another is a familiar historical event, but power diffusion is a more novel process. The problem for all states in today's global information age is that more things are happening outside the control of even the most powerful states. In the words of a former State Department director of policy planning, 'the proliferation of information is as much a cause of nonpolarity as is the proliferation of weaponry.' "

pessoas conectadas, e manipulando o funcionamento de inúmeras máquinas e equipamentos digitais, representa uma difusão de poder inédita na história.

> O poder baseado em fontes de informação não é novo, mas o ciberpoder é. Há muitas definições para Ciberespaço mas, em termos gerais, 'ciber' é um prefixo que se refere a atividades eletrônicas e computação. E desta maneira temos uma definição: 'o Ciberespaço é um domínio operacional caracterizado pelo uso da eletrônica para ... manipular a informação via sistemas interconectados e suas infraestruturas associadas". O poder depende do contexto e o ciberpoder depende dos recursos que caracterizam o domínio do ciberespaço.
>
> [...] ciberpoder é a capacidade de se obter os resultados desejados através do uso de fontes de informação eletronicamente interconectadas dentro do domínio cibernético. Numa definição mais amplamente utilizada, ciberpoder é 'a capacidade de se utilizar o Ciberespaço para criar vantagens e influenciar eventos em outros ambientes operacionais e através dos instrumentos de poder'. O ciberpoder pode ser utilizado para obter resultados dentro do Ciberespaço ou fazer uso de ciberrecursos para alcançar resultados em outros domínios fora do Ciberespaço.
> (NYE JR, 2011, p. 1) [39]

O neoliberalismo acredita que a expansão do comércio e da economia liberal são a base para o desenvolvimento de interdependências sociais dinâmicas e diversificadas que levarão à melhoria das condições de vida de uma quantidade crescente de pessoas. Na Era da Informação, quando o Ciberespaço atua como um mediador cada vez mais poderoso e pervasivo, viabilizando a comunicação entre pontos cada vez mais variados e remotos do planeta, as interdependências complexas da globalização neoliberal acontecem através de sistemas digitais e cabos óticos que transmitem informações na velocidade da luz. Neste contexto, analisa NYE JR, a informação digitalizada em si assume uma proeminência ímpar e por isso o seu controle representa o que de mais efetivo o Ciberespaço tem a oferecer como um instrumento de poder.

39 tradução nossa, do original: "Power based on information resources is not new; cyber power is. There are dozens of definitions of cyberspace but generally “cyber” is a prefix standing for electronic and computer related activities. By one definition: “cyberspace is an operational domain framed by use of electronics to …exploit information via interconnected systems and their associated infra structure.” Power depends on context, and cyber power depends on the resources that characterize the domain of cyberspace.

[...] cyber power is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain. In one widely used definition, cyber power is “the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power.” Cyber power can be used to produce preferred outcomes within cyberspace or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace."

2.3 O Poder Cibernético na Visão de Joseph Nye Jr

A parte anterior deste trabalho apresentou algumas visões contrastantes sobre as possibilidades que o Ciberespaço oferece em termos de conflito de poder. Entretanto, uma questão importante ainda persiste: quais bases teóricas poderiam ser utilizadas para identificar e analisar o efetivo exercício de poder no Ciberespaço ? O trabalho entitulado 'O Poder Cibernético' de NYE JR (2011) oferece diversos subsídios neste sentido partindo da visão neoliberal do sistema internacional para tentar compreender as peculiaridades do ambiente cibernético.

Inicialmente é importante retomar a definição neoliberal de poder dentro do Ciberespaço enfatizando os aspectos relativos ao seu efetivo exercício: no domínio cibernético o poder é quase sempre exercido de maneira indireta através da manipulação ou apropriação (ilícita ou não) de informações que irão posteriormente orientar decisões estratégicas, controlar o funcionamento de sistemas específicos ou influenciar o comportamento de pessoas. Uma vez que o Ciberespaço é essencialmente um transmissor de mensagens eletrônicas digitais, a intervenção neste meio envolve o uso de ferramentas programacionais ou equipamentos eletrônicos que sejam capazes de interagir com seus diferentes sistemas e redes. O autor explicita: "[...] o poder cibernético é a habilidade de se obter os resultados desejados através do uso de informações eletronicamente interconectadas dentro do domínio cibernético [...]" (NEY JR, 2010, p. 3) [40], permitindo assim distinguir a ação no meio cibernético das ações em outros domínios distintos ao mesmo tempo em que aponta sua característica mais significativa: a manipulação de informações em meio digital visando a obtenção de resultados pré-definidos dentro ou fora do ciberdomínio.

NEY JR também faz distinção entre o "poder rígido" (*hard power*) e o "poder suave" (*soft power*), e estes conceitos encontram muitas aplicações nos tipos de ações possíveis dentro do domínio cibernético, uma vez que os meios para se manipular a informação dentro do Ciberespaço são muito variados e vão desde a modificação no funcionamento de sistemas digitais que controlam recursos físicos militares, como armamentos e indústrias, até intervenções mais sutis como a implantação de ideias favoráveis a determinados interesses e o direcionamento da opinião pública.

40 tradução nossa, do original: "[...] cyber power is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain [...]"

> A evolução das definições modernas de ciência social para o poder comportamental é algumas vezes resumida como as "três faces do poder". O primeiro aspecto ou "face" do poder foi definido por Robert Dahl nos seus estudos em New Haven durante a década de 1950. O seu trabalho sobre como conseguir que as pessoas façam coisas que, de outra maneira, elas não fariam é amplamente utilizado hoje em dia [como definição de poder], apesar de abranger apenas parte do poder comportamental. Entretanto, na década de 1960 os cientistas políticos Peter Bachrach and Morton Baratz chamaram a atenção para o fato de que o trabalho de Dahl não abordava o que eles entendiam como sendo a "segunda face do poder", a dimensão da opacidade, ou seja: a capacidade de ocultar o exercício do poder de tal forma que a coerção não se torne clara ou visível. Por fim, na década de 1970, o sociólogo Steven Lukes afirmou que ideias e crenças também ajudam a moldar as preferências das pessoas e, por isso, o poder também pode ser exercido pela indução do desejo nos outros. [A partir destes estudos], na década de 1990, eu fiz a distinção entre poder "rígido" e "suave" dentro de uma escala de intensidade que vai desde a ordem de comando até a cooperação voluntária. O poder "rígido" (hard power) se baseia na coerção e no poder financeiro, enquanto o poder "suave" (soft power) acontece através da opacidade, atração ou persuasão. (NYE JR, 2010, p. 2) [41]

Paralelamente a este conceito de ação existem também dois níveis estruturais básicos no Ciberespaço que, devido às suas peculiaridades técnicas, limitam naturalmente os tipos de intervenção possíveis.

O primeiro deles, chamado de "nível físico" ou "infraestrutura", está relacionado com os recursos tangíveis que compõem as redes de dados digitais por onde trafegam as informações cibernéticas (roteadores de altíssima velocidade e largura de banda, milhares de quilômetros de cabos óticos reforçados, etc). O enorme custo de aquisição e manutenção destes equipamentos eletrônicos muito específicos, além do fato deles ocuparem espaços geográficos bem definidos, faz com que sejam necessariamente propriedade de Estados ou de grandes grupos empresariais, o que consequentemente os transforma em recursos físicos submetidos a uma soberania específica que pode, seguindo interesses próprios, utilizá-los para restringir ou definir conteúdos, manipulando desta forma o acesso às informações disponíveis no Ciberespaço.

41 tradução nossa, do original: "The evolution modern social science definitions of behavioral power is sometimes summarized as “the three faces of power.” The first aspect or “face” of power was defined by Robert Dahl in studies of New Haven in the 1950s. His focus on getting others to do what they would not otherwise do is widely used today even though it covers only part of power behavior. In the 1960s, the political scientists Peter Bachrach and Morton Baratz pointed out that Dahl’s definition missed what they called the “second face of power,” the dimension of agenda setting, or framing issues in such a way that the issue of coercion never arose. In the 1970s, the sociologist Steven Lukes pointed out that ideas and beliefs also help shape others’ preferences, and one can also exercise power by determining others’ wants. In 1990, I distinguished hard and soft power along a spectrum from command to co-optive behavior. Hard power behavior rests on coercion and payment. Soft power behavior rests on framing agendas, attraction or persuasion."

> Devido ao fato dos componentes físicos que compõem a infraestrutura da internet estarem situados em pontos específicos do planeta, e os governos serem soberanos sobre espaços geográficos, a localização é um recurso importante do ciberespaço. Os governos podem tomar iniciativas para subsidiar infraestrutura, educação digital e proteção de propriedade intelectual que irão encorajar ou (desencorajar) o desenvolvimento de determinadas capacidades dentro das suas fronteiras [...]
> (NEY JR, 2010, p. 9) [42]

Neste sentido é bem conhecida a atitude de censura e controle de acesso a conteúdos disponíveis na internet empreendida por países com governos autoritários. Menos conhecida, por outro lado, é a filtragem ou redirecionamento sutil de informações para o grande público realizados pelos EUA e vários países europeus.

> Segundo a 'Open Net Initiative', pelo menos 40 países adotam políticas altamente restritivas e equipamentos específicos (firewalls) para evitar a discussão de conteúdos considerados indesejados [na internet]. Dezoito países realizam uma censura política que é descrita como 'invasiva' na China, Vietnam e Iran e 'significativa' na Líbia, Etiópia e Arábia Saudita. Mais de 30 Estados realizam filtragem de conteúdo por motivos sociais, bloqueando o acesso a assuntos como sexo, jogo e drogas. Mesmo os EUA e muitos países europeus realizam este procedimento de maneira "seletiva". Algumas vezes isto é aceito e outras não. Se a filtragem de conteúdo é realizada de maneira oculta, torna-se muito difícil para o cidadão comum descobrir o que ele não sabe que existe [...] (NEY JR, 2010, p. 8) [43]

A atuação no nível físico, devido às suas características próprias e equipamentos envolvidos, está restrita aos governos e ao grande interesse econômico, e oscila segundo as tendências políticas e de mercado, caracterizando-se pelo uso da força coerciva (militar ou policial), legal (legislação específica) e da tecnologia de ponta (supercomputadores e grandes bancos de dados) para controlar ou orientar o uso do ciberespaço.

Exemplos claros deste tipo de poder podem ser vistos nas prisões ou perseguições de pessoas que publicam conteúdo considerado proibido no Ciberespaço (pedofilia e quebra de direitos autorais por exemplo) (HARMON, 2003),

42 tradução nossa, do original: "Because the physical infrastructure of the internet remains tied to geography and governments are sovereign over geographical spaces, location still matters as a resource in the cyber domain. Governments can take steps to subsidize infrastructure, computer education, and protection of intellectual property that will encourage (or discourage) the development of capabilities within their borders [...]"

43 tradução nossa, do original: "According to the Open Net Initiative, at least 40 countries use highly restrictive filters and firewalls to prevent the discussion of suspect materials. Eighteen countries engage in political censorship, which is described as “pervasive” in China, Vietnam and Iran, and “substantial” in Libya, Ethiopia, and Saudi Arabia. More than 30 states filter for social reasons, blocking content related to topics such as sex, gambling and drugs. Even the United States and many European states do this “selectively.” Sometimes this is accepted and sometimes not. If the filtering is secretive, it is hard for citizens to know what they do not know [...]"

na desativação de sítios digitais (*sites*) pelos mesmos motivos (PFANNER, 2010), nos esforços de censura e monitoração de usuários existentes em países como China e Irã (SCHMIDT; COHEN, 2014), e também na "publicidade inteligente" que utiliza a inteligência artificial e bancos de dados de grande porte para armazenar os hábitos dos internautas visando incluir, nas páginas que eles acessam, determinados anúncios que possuem maior probabilidade de induzi-los ao consumo (MANJOO, 2014).

O segundo nível, chamado de "nível virtual", diferencia-se muito do primeiro tanto nos tipos de atores que se beneficiam com as suas peculiaridades quanto nos tipos de ação possíveis. Isto acontece devido ao baixo custo e à grande disponibilidade de aplicativos (incluindo aqueles específicos para ataques virtuais), além da facilidade de publicação de conteúdo e interação com outros internautas, características que oferecem ao usuário comum e aos pequenos grupos organizados uma significativa capacidade de intervenção e influência no domínio cibernético.

> [...] as barreiras para se acessar o ciberespaço são tão pequenas [hoje em dia] que atores não estatais e pequenos Estados podem exercer papéis significativos com custos muitos baixos. Ao contrário do mar, ar e espaço sideral; o ciberespaço compartilha, em termos até bem mais amplos, três características com a guerra terrestre: o número de participantes, facilidade de entrada e oportunidades de ocultação ... Em terra, o domínio não é uma vantagem de fácil obtenção [...]
> (NEY JR, 2010, p. 4) [44]

Ações perniciosas como a implantação de programas maliciosos em computadores de terceiros ("vírus de computador"), monitoração de pessoas, espionagem de empresas, propaganda extremista, doutrinamento ideológico e até mesmo pequenos ataques capazes de causar danos físicos estão ao alcance dos usuários comuns no nível virtual da internet. Para cada uma destas atividades existem ferramentas programacionais de fácil acesso disponíveis em sites especializados, e o uso da maioria delas não exige maiores conhecimentos além da utilização básica da internet.

> Este é um exemplo sobre como as ferramentas cibernéticas estão confundindo as linhas de ação que separam as empresas com grande capacidade técnica e os atores com recursos limitados [...] os indivíduos podem atuar sem dificuldade no domínio cibernético devido ao seu baixo custo de entrada, largas possibilidades de ocultação e facilidade de saída.

44 tradução nossa, do original: "[...] the barriers to entry in the cyber domain are so low that non-state actors and small states can play significant roles at low levels of cost. In contrast to sea, air and space, cyber shares three characteristics with land warfare – though in even greater dimensions: the number of players, ease of entry, and opportunity for concealment…On land, dominance is not a readily achievable criterion [...]"

> Algumas vezes eles agem com consentimento governamental e outras contra o governo. Por exemplo: antes do ataque russo à Georgia em 2008, qualquer civil russo ou aspirante a guerreiro cibernético podia visitar um sítio simpatizante da causa russa e baixar o programa e as instruções necessárias para lançar um ataque de 'Negação de Serviço' ou 'Denial of Service' (DOS) contra a Georgia. Durante os protestos populares no Iran em 2009, o Twitter e as redes sociais foram essenciais para organizar e divulgar os protestos. [Durante este período] o governo dos EUA pediu aos executivos do Twitter que não tirassem o seu sítio do ar para a manutenção de rotina programada. Os norte-americanos temiam que a interrupção atrapalhasse as passeatas. Em represália, seis meses depois um grupo autointitulado 'Exército Cibernético Iraniano' conseguiu redirecionar o tráfico endereçado ao Twitter para uma página contendo slogans antiamericanos. Em fevereiro de 2010 o governo iraniano bloqueou a maior parte do acesso ao Twitter e vários outros sítios semelhantes (NEY JR, 2010, p. 13) [45]

Ataques de "Negação de Serviço" (*Denial of Service,* abreviado como DoS) é um tipo de conflito cibernético muito comum e utilizado por diversos tipos de atores devido à sua facilidade de implementação e alto índice de sucesso. Ele se consiste em utilizar programas específicos, facilmente encontrados na internet, capazes de realizar uma grande quantidade de chamadas seguidas a um determinado servidor (computador ligado à internet que disponibiliza uma ou várias páginas digitais) dentro de um intervalo bem curto de tempo, sobrecarregando o acesso e impedindo que outras pessoas acessem este computador onde a empresa-alvo alocou a sua página ou sítio digital. Este tipo de ataque acontece com muita frequência e mesmo nas suas versões mais sofisticadas (chamadas de DDoS - *Distributed Denial of Service* - ou 'Negação de Acesso Distribuída') pode ser realizado por usuários com conhecimentos mínimos sobre a internet e seus aplicativos (SHANDKDHAR, 2016).

O nível virtual tem sido de grande utilidade também para grupos pequenos em busca de visibilidade para a sua causa ou ideologia. É bem conhecida atualmente a maneira como a organização terrorista "Al Qaeda" usou a internet para se expandir pelo mundo, aumentando significativamente sua área de influência e quantidade de seguidores.

45 tradução nossa, do original: "This is an example of how cyber tools begin to blur the lines between organizations with highly structured networks and individuals with lightly structured networks [...] individuals can easily play in the cyber domain because of the low cost of investment for entry, virtual anonymity, and ease of exit. Sometimes they act with government approval and sometimes against them. For example, before the 2008 Russian attack on Georgia, any civilian, Russian born or otherwise, aspiring to be a cyber warrior was able to visit pro-Russia websites to download the software and instructions necessary to launch denial of service attacks on Georgia. During student protests in Iran in 2009, Twitter and social networking sites were crucial for organizing and reporting demonstrations. The U.S. government asked Twitter executives not to take the site down for scheduled maintenance. They were worried that might interfere with how Twitter was being used to organize demonstrations. Six months later, however, an unknown group called the Iranian Cyber Army successfully redirected Twitter traffic to a website with an anti-American message, and in February 2010, the Iranian government blocked most access to Twitter and other sites."

> Graças às ferramentas cibernéticas a 'Al Qaeda' tem sido capaz de se expandir saindo de uma organização hierárquica restrita a células geograficamente estruturadas para uma rede mundial na qual os voluntários podem se autorecrutar. Conforme descreve um especialista em terrorismo: "o principal local de radicalização não é o Paquistão ou o Iemen ... Mas sim uma solitária experiência de comunidade virtual: a 'ummah' na internet"
> (NEY JR, 2010, p. 13) [46]

Todo este poder, entretanto, encontra limites diante do esforço de controle exercido pelos governos e grandes empresas. Apesar de reduzir consideravelmente a assimetria entre os pequenos e grandes atores, o nível virtual não os nivela, e por isso a capacidade coerciva técnica e operacional do poder instituído tende a prevalecer no ciberespaço.

> É digno de nota que os atores individuais se beneficiam de vulnerabilidades assimétricas no domínio cibernético quando comparados com governos e grandes organizações. Eles necessitam de um investimento muito pequeno e têm muito pouco a perder ao entrar e sair [do ciberespaço]. A grande vulnerabilidade que eles possuem é a coerção legal e ilegal que podem sofrer das autoridades se forem descobertos, mas apenas um pequeno percentual destes atores são efetivamente identificados e incriminados. Por outro lado, as empresas possuem grandes vulnerabilidades devido aos vultosos investimentos feitos em sistemas operacionais complexos, em propriedade intelectual e reputação no mercado. Da mesma maneira, os governos também dependem de sistemas complexos [em infraestrurura] que podem ser facilmente interrompidos ou danificados, [além de serem vulneráveis a] instabilidades políticas e [ameaças ao seu] poder de influência (*soft power*). Ao mesmo tempo em que os pequenos ataques empreendidos por indivíduos dificilmente subjugarão governos ou grandes empresas, eles podem impor danos consideráveis ao comprometerem serviços ou reputações, tudo isso utilizando investimentos mínimos.
> (NEY JR, 2010, p. 13) [47]

Observamos então que os conceitos de poder rígido (*hard power*) e suave (*soft power*), atuando tanto a nível físico quanto virtual, nos permitem agrupar de maneira clara e didática os tipos de ações empreendidas pelos atores cibernéticos voltadas para o efetivo exercício de poder em vários níveis.

46 tradução nossa, do original: "Thanks to cyber tools, Al Qaeda has been able to move from a hierarchical organization restricted to geographically organized cells to a horizontal global network to which local volunteers can self-recruit. As one expert on terrorism describes: 'the key place for radicalization is neither Pakistan nor Yemen nor Afghanistan … but in a solitary experience of a virtual community: the ummah on the Web'."

47 tradução nossa, do original: "It is worth noting that individual actors in the cyber domain benefit from asymmetrical vulnerability compared to governments and large organizations. They have very low investment and little to lose from exit and re-entry. Their major vulnerability is to legal and illegal coercion by governments and organizations if they are apprehended, but only a small per cent are actually caught. In contrast, corporations have important vulnerabilities because of large fixed investments in complex operating system, intellectual property, and reputation. Similarly, large governments depend on easily disrupted complex systems, political stability, and reputational soft power. While hit and run cyber strikes by individuals are unlikely to bring governments or corporations to their knees, they can impose serious costs of disruption to operations and to reputations with a miniscule investment [...]"

Quadro 1 - Dimensões física e virtual do poder cibernético

	DENTRO do ciberespaço	FORA do ciberespaço
físico	**Hard**: controle governamental ou pressões sobre empresas e provedores, firewalls, filtros de conteúdo **Soft**: infraestrutura beneficiando determinados grupos	**Hard**: destruição de roteadores e cabos, prisão de ativistas, ameaças a bloggers **Soft**: campanhas para prejudicar provedores
virtual	**Hard**: ataques de negação de serviço (DOS), malwares **Soft**: definição de normas e padrões digitais, restrições em mecanismos de busca	**Hard**: ataques contra instalações industriais **Soft**: manipulação da opinião pública, estímulo a preferências, normas de rejeição

Fonte: NEY JR (2010, p. 5) [48]

Uma outra maneira de se agrupar os tipos de ação cibernética é observá-los segundo a relação de influência estabelecida, orientando-se pelas "três faces do poder" comportamental:

Quadro 2 - As três faces do poder no domínio cibernético

	***A* induz *B* a fazer coisas que inicialmente não faria**	***A* reduz as opções de ação para *B***	***A* orienta as ações de *B***
HARD	ataques DOS, malwares, prisão de ativistas, ataques industriais	firewalls, filtros de conteúdo e pressões sobre empresas	ameaças de punição a bloggers
SOFT	manipulação de opinião	regras e padrões, restrições em mecanismos de busca	estímulo a preferências (nacionalismo, etc), normas de rejeição (pornografia infantil)

Fonte: NEY JR (2010, p. 7) [49]

Além de tipos variados de ação, a redução de assimetria proporcionada pelo ambiente cibernético possibilita também a existência de uma gama bem diversificada de atores, e por isso a identificação dos seus tipos e respectivas possibilidades é importante para a compreensão sobre como o poder pode ser exercido no Ciberespaço. Afirma NYE JR ao se referir a esta diversidade: "A difusão de poder no domínio cibernético é representada por um número de atores e a relativa redução das diferenças de poder entre eles. Qualquer ator, desde um 'hacker' adolescente até um Estado, pode causar danos [a outrem] no Ciberespaço. Conforme afirmou jocosamente certa vez uma charge na revista 'The New Yorker': 'na internet, ninguém sabe se você é um cachorro' " (2010, p. 9) [50]. De fato, é surpreendente a extensão dos danos que um ator aparentemente insignificante é

48 tradução nossa, do original: "Table 1: Physical and Virtual Dimensions of Cyber Power"

49 tradução nossa, do original: " Table 2: Three Faces of Power in the Cyber Domain"

50 tradução nossa, do original: " The diffusion of power in the cyber domain is represented by the vast number of actors, and relative reduction of power differentials among them. Anyone from a teen age hacker to a major modern government can do damage in cyber space, and as the famous New Yorker cartoon once put it, “on the internet, no one knows you are a dog. [...]"

capaz de empreender no Ciberespaço. Mesmo com os recursos mais modernos de segurança digital sendo constantemente renovados e aprimorados, as ameaças continuam a existir se adaptando às novas políticas de proteção implementadas.

> [...] o infame vírus [de computador chamado] 'Love Bug', criado por um 'hacker' nas Filipinas, causou um prejuízo estimado em U$$ 15 bilhões; redes de computadores essenciais para as forças armadas dos EUA são atacadas centenas de milhares de vezes todo o dia; calcula-se que grupos criminosos cibernéticos tenham roubado cerca de U$$ 1 trilhão em segredos industriais e propriedade intelectual durante o ano de 2008; descobriu-se que somente uma rede de espionagem cibernética, chamada 'GhostNet', conseguiu infectar 1295 computadores em 103 países, sendo que 30% deles eram alvos governamentais de grande valor; grupos terroristas utilizam a internet para recrutar novos membros e planejar ações [ao redor do mundo]; ativistas políticos e ambientais [utilizam a internet] para interromper o funcionamento de diversos endereços eletrônicos pertencentes a empresas e governos. O que é significativo sobre o [exercício do] poder no domínio cibernético não é o fato de que os governos não participam dele, conforme acreditavam os primeiros [teóricos] libertários sobre o funcionamento da internet, mas sim os [variados] recursos de poder disponíveis a diferentes atores e a redução das diferenças entre as possibilidades [de ação] de atores estatais e não estatais em muitas situações [...]" (NEY JR, 2010, p. 9) [51]

Os atores no Ciberespaço podem ser separados em três grandes grupos considerando-se as suas semelhanças em termos de capacidade de ação:

Quadro 3 - Os atores e suas fontes de poder no Ciberespaço

ator	poderes	vulnerabilidades
Governos	● Construção e manutenção da infraestrutura física ● Definição das regras de uso e de propriedade intelectual ● Coerção legal e física de indivíduos ● Controle de acesso ao seu mercado interno ● Recursos para ataque e defesa cibernéticas ● Definição da legislação dentro do seu território ● Confiança dos eleitores gerando capacidade de convencimento e cooptação (soft power)	● Grande dependência de sistemas complexos de infraestrutura cujo funcionamento pode ser facilmente interrompido ● Estabilidade política ● Manutenção de boa reputação pelas figuras públicas
Organizações de Grande Porte	● Grande disponbilidade de orçamento e recursos humanos ● Atuação transnacional ● Alto controle do seus códigos e produtos desenvolvidos ● Reputação da marca no mercado gerando capacidade de influência sobre as pessoas (soft power)	● Disputas judiciais com grande impacto financeiro ● Roubo de propriedade intelectual ● Interrupção no funcionamento dos seus sistemas ● Perda de reputação no mercado
Indivíduos e Organizações de Pequeno Porte	● Baixo custo de investimento para atuação no Ciberespaço ● Anonimato e facilidade para saída do sistema ● vulnerabilidade assimétrica se comparados com outros atores mais poderosos	● Coerção legal e física caso seja identificado

Fonte: NEY JR (2010, p. 10) [52]

51 tradução nossa, do original: "[...] The infamous “Love Bug” virus unleashed by a hacker in the Philippines is estimated to have caused $15 billion in damage. Computer networks essential to the American military are attacked “hundreds of thousands of times every day”. Cybercriminal groups were said to have stolen over $1 trillion in data and intellectual property in 2008. One cyber espionage network — GhostNet — was found to be infecting 1,295 computers in 103 countries, of which 30 percent were high value governmental targets. Terrorist groups use the web to recruit new members and plan campaigns. Political and environmental activists disrupt web sites of companies and governments. What is distinctive about power in the cyber domain is not that governments are out of the picture as the early cyber libertarians predicted, but the different power resources that different actors possess, and the narrowing of the gap between state and non state actors in many instances [...]"

52 tradução nossa, do original: "Table 3: Relative Power Resources of Actors in the Cyber Domain"

Além dos poderes descritos acima é importante acrescentar que vários países possuem grupos militares especializados em realizar ataques cibernéticos. O crescente reconhecimento do Ciberespaço como um domínio independente e altamente estratégico pelas forças armadas tem levado à percepção de que, no campo de batalha digital, não basta ser capaz de se proteger, é imprescindível saber atacar com eficiência. Afirma NYE JR (2010, p. 10): "[...] os governos também possuem capacidades ofensivas no ciberespaço. Por exemplo: a 'Décima Frota Norte-Americana' ou a 'Vigésima Quarta Força Aérea' não possuem navios ou aviões, o campo de batalha destas forças militares é o Ciberespaço [...]" [53]. Entretanto, uma vez que o domínio virtual é apenas o meio de transmissão das informações e não o alvo final da maioria dos ataques, os militares costumam considerá-lo preponderantemente como um auxiliar aos combates no mundo físico.

> [...] muitos especialistas veem o ataque cibernético muito mais como um importante auxiliar à guerra entre os Estados do que como uma arma de destruição em massa (conforme as armas atômicas). Os Estados invadem os seus respectivos sistemas computacionais como uma 'preparação do campo de batalha' visando possíveis conflitos futuros. Tanto teóricos militares norte-americanos como os chineses têm discutido esses passos mas muito pouco é divulgado publicamente sobre doutrinas ofensivas no ciberespaço [...]" (NEY JR, 2010, p. 11) [54]

A soberania que os governos possuem sobre os seus respectivos territórios e o rígido controle que as grandes corporações mantém sobre as redes e equipamentos digitais dos quais são proprietárias têm como consequência uma distribuição irregular e muitas vezes competitiva do controle exercido sobre as atividades no ambiente cibernético. Embora a nível virtual exista um alto grau de liberdade nas interações transnacionais e intersistêmicas, no nível de infraestrutura há muitas partes no Ciberespaço com governança definida e bem identificada, onde as ações de atores externos são restritas ou cuidadosamente controladas. Estas duas realidades antagônicas e sobrepostas fazem com que o controle de conteúdo no ambiente virtual seja sempre fugidio e mutante.

53 tradução nossa, do original: "[...] Governments also have the capacity to carry out offensive cyber attacks. For example, America's Tenth Fleet and Twenty-fourth Air Force have no ships or planes. Their battlefield is cyberspace [...]'

54 tradução nossa, do original: "[...] Most experts see cyber attack as an important adjunct rather than an overwhelming weapon (unlike nuclear) in inter-state wars. States intrude into each others' cyber systems in "preparation of the battlefield" for what could be future conflicts. Both American and Chinese military theorists have discussed such steps, but little is publicly stated about offensive cyber doctrines [...]"

> [...] Alguns veem o Ciberespaço como uma 'terra sem lei' semelhante ao velho oeste [dos filmes norte-americanos], mas na prática ele possui muitas áreas de governança tanto públicas quanto privadas [...] A governaça imperfeita do Ciberespaço pode ser classificada como um regime complexo de instituições e normas fracamente acopladas; algo entre uma instituição integrada, que impõe regras através de sua estrutura hierárquica, e práticas altamente fragmentadas sem qualquer coesão discernível.
> (NEY JR, 2010, p. 14) [55]

Em termos de governança o Ciberespaço representa uma relação dinâmica e instável entre uma grande quantidade de interesses divergentes e simultâneos, tendo como elementos principais, de um lado, o desejo de controle, oriundo dos grandes grupos de poder que nele atuam, e de outro, a liberdade de ação e interação exigida para que aconteça uma conexão remota efetiva entre atores muito variados. É no tráfego livre, cada vez mais intenso e rápido da informação ao redor do mundo, que se realiza o motivo maior para a existência do meio cibernético. Mutuamente interdependentes através das miríades de caminhos digitais, a maior parte dos seus atores não seria capaz de se desconectar sem sofrer graves prejuízos em termos comerciais e econômicos, além de ter a sua presença no cenário internacional severamente restrita ou anulada.

> [...] afirma-se que a China, por exemplo, tem controlado o desenvolvimento das suas empresas por trás dos seus 'firewalls' [sistemas de segurança locais], de maneira que possa se desconectar [facilmente] da internet global caso seja atacada. Por outro lado, a China - entre outros governos - busca intensamente os benefícios da conectividade [internacional]. A tensão [entre estes dois extremos] leva a compromissos imperfeitos.
> (NEY JR, 2010, p. 16) [56]

Dentro da visão neoliberal a interdependência complexa global tende a criar laços cada vez mais diversificados em vários níveis de intensidade entre os Estados, reforçando, desta forma, a dependência das nações entre si e a dependência mundial do principal meio moderno de viabilização deste processo: o Ciberespaço. Ao se tornar um meio de uso intenso por parte de todos os países neste início do século XXI, o Ciberespaço tende a ser visto em termos de governança

55 tradução nossa, do original: "Some see cyberspace as analogous to the ungoverned lawless Wild West, but in practice there are many areas of private and public governance [...] The imperfect governance of cyberspace can be categorized as a “regime complex” of loosely coupled norms and institutions somewhere between an integrated institution that imposes regulation through hierarchical rules, and highly fragmented practices and institutions with no identifiable core and non-existent linkages."

56 tradução nossa, do original: "[...] China, for example, is described as developing its own companies that it can control behind its firewall, and planning to disconnect from the global Internet if it is attacked. Nonetheless, China — and other governments — still seek the economic benefits of connectivity. The tension leads to imperfect compromises."

como um bem ou recurso comum. Afirma NYE JR (2010, p. 15): "o Ciberespaço pode ser categorizado como o que Elinor Ostrom chamou de 'recurso de uso comum', um meio do qual a exclusão é difícil e a exploração exclusiva por uma parte subtrai valor para as outras partes [...]" [57] Neste sentido é importante enfatizar que, por motivos políticos e de cultura de uso, a propriedade dos recursos tangíveis pertinentes ao nível físico do Ciberespaço não implica necessariamente em controle sobre o nível virtual. A utilização simultânea destes recursos em termos mundiais faz com que a existência de restrições excessivas atendendo a interesses pontuais torne o uso compartilhado inviável ou indesejável por parte de outros interesses.

A percepção da importância do Ciberespaço como um recurso único e comum também torna improvável, no caso de uma guerra cibernética de grande escala, que haja interesse na sua destruição ou na interrupção do seu funcionamento porque qualquer prejuízo maior ao tráfego globalizado de informações trará um enorme prejuízo à economia e à vida social da maior parte dos países modernos.

> [...] mesmo quando o responsável por um ataque consegue se ocultar com eficiência, os outros governos podem estar presos a relações recíprocas de interdependência tão intensas que a realização de um ataque de grandes proporções se torne contraprodutiva. Diferente das alianças bipolares mudiais que dividiram a interdependência militar durante a Guerra Fria, atualmente países como EUA, China e outros estão interconectados por múltiplas redes. A China, por exemplo, iria perder muito com um ataque que prejudicasse severamente a economia estadunidense e vice-versa. (NEY JR, 2010, p. 16) [58]

A interdependência complexa mundial mediada pelo Ciberespaço aliada a uma assimetria de ação que favorece aos atores mais fracos é o ponto principal do pensamento de NYE JR sobre o exercício de poder no meio cibernético. A capacidade que um grande número de atores possuem para influenciar pessoas, grupos e governos a nível mundial e em graus variados de intensidade confere ao meio cibernético um *status* totalmente diferenciado ao ser comparado com outros espaços de poder. NYE JR não acredita que o Ciberespaço venha a igualar assimetrias em algum momento, mas afirma claramente que a sua existência proporciona uma difusão de poder inédita na existência humana (NYE JR, 2010, p. 19).

57 tradução nossa, do original: "Cyber space can be categorized as what Elinor Ostrom terms a “common pool resource” from which exclusion is difficult and exploitation by one party can subtract value for other parties [...]"

58 tradução nossa, do original: "[...] Even when the source of an attack can be successfully disguised under a “false flag,” other governments may find themselves sufficiently entangled in interdependent relationships that a major attack would be counterproductive. Unlike the single strand of military interdependence that linked the U.S. and the Soviet Union in the Cold War, the United States, China, and other countries are entangled in multiple networks. China, for example, would itself lose from an attack that severely damaged the American economy, and visa versa."

CAPÍTULO III

ESTUDO DE CASO: GEÓRGIA

3.1 Introdução

A Geórgia é um país situado no Cáucaso e que faz fronteira com a Rússia, Turquia, Armênia e Azerbaijão. Em 1921 foi anexado à URSS através de uma invasão militar russa e se manteve fortemente vinculado tanto política quanto economicamente ao bloco soviético até 1991, quando reconquistou sua independência após o fim da Guerra Fria e da bipolaridade que a caracterizou (Government of Georgia, 2014).

O rompimento dos laços de dependência com a Rússia representou para a Geórgia o surgimento e a consolidação de uma nova política de Estado identificada com a economia de mercado e aos valores capitalistas, o que levou o país a uma crescente reaproximação com o ocidente e, consequentemente, a um rápido desenvolvimento econômico e social devido ao significativo incremento nas suas relações comerciais com a Europa e os EUA (IEG, 2009). Entretanto, este tipo de orientação política começou a incomodar à Rússia porque trouxe a esfera de influência dos EUA para a sua fronteira e, pior ainda, para uma região estratégica em termos de transporte de petróleo para o ávido mercado consumidor europeu, do qual a economia russa é muito dependente (BLUM, 2002). A antipatia de Moscou às tendências político-comerciais da Georgia, aliada ao crescimento dos interesses ocidentais na região, levou a OTAN a considerar a entrada da Geórgia para o seu acordo de proteção mútua através de negociações que começaram logo após a independência do país e se intensificaram com a ascensão do novo governo pró-ocidente em 2003 (NATO, 2017), uma manobra política com desdobramentos militares que dificultou ainda mais as relações com a Rússia.

Em 2006 a inauguração do oleoduto Baku–Tbilisi–Ceyhan, o segundo maior de toda a região, uma iniciativa conjunta da Georgia, Turquia e Azerbaijão (BAYATLI, 2006, p. 92-95), levou a insatisfação russa a um estado de paroxismo. Esta nova linha de transmissão cujo objetivo é levar o petróleo do Mar Cáspio para o Mediterrâneo representa, na prática, um caminho alternativo aos oledutos russos que até então eram os únicos a realizar este tipo de operação na região.

Esta nova opção de transmissão é estratégica para o ocidente porque reduz sobremaneira a dependência que os EUA e Europa tinham de Moscou para conseguir acessar as enormes reservas petrolíferas situadas na Ásia Central. A quebra no monopólio de exportação petrolífera da Rússia por parte da Geórgia e o impacto financeiro e político que este fato gerou no comércio internacional para Moscou colaborou consideravelmente com o surgimento de um estado crescente de tensão nas relações entre os dois países e gerou uma crise diplomática que representou mais um forte estímulo ao conflito de 2008 (MOUAWAD, 2008).

Paralelamente aos conflitos de interesse comercial com a Rússia, a Geórgia também enfrenta conflitos internos devido à heterogeneidade de etnias que o seu território abriga. Dentre elas, destaca-se para a guerra de 2008 entre a Rússia e a Geórgia o grupo humano que ocupa a região da Ossétia. Os ossetianos, cujo território norte pertence à federação russa e o território sul está situado dentro dos limites geográficos da Geórgia, são um grupo étnico-linguístico com raízes situadas na região do Irã (TOPCHISHVILI, 2009) e que atualmente sofre grande influência do governo russo. Não somente porque a Ossétia do Norte é um Estado da Rússia, mas também pelo fato da Ossétia do Sul reivindicar sua independência desde 1991 (mesma época da independência da Geórgia) e receber amplo apoio russo neste sentido (BBC News, 2016).

A primeira guerra separatista aconteceu no período de 1991 a 1992 e terminou com um cessar fogo mediado pelos russos. Nos anos que se seguiram o governo provisório da Ossétia do Sul e o governo da Geórgia, sempre com a mediação de Moscou, realizaram várias conversações buscando obter uma solução política para a região mas nenhum acordo definitivo foi alcançado. A prolongada indefinição para a situação da Ossétia do Sul (16 anos de negociações mal sucedidas entre o conflito de 1992 e o de 2008) terminou por incentivar diversos tipos de comércios ilegais, sequestros e contrabandos na região, além de escaramuças eventuais entre grupos paramilitares separatistas e o exército da Geórgia, agravando cada vez mais o problema e ampliando grandemente as suas consequências perniciosas para os âmbitos social e econômico (DARC, 2009).

Por fim, em 2008, a escalada de tensão entre os governos da Rússia e da Geórgia causada pelo intenso conflito de interesses comerciais entre os dois países,

junto com o crescimento dos embates entre os grupos separatistas da Ossétia do Sul e o exército da Geórgia levaram a uma guerra que envolveu diretamente a Rússia, o território da Ossétia do Sul e a Geórgia.

3.2 O Conflito

Antecipando-se aos ataques das forças militares, aparentemente realizando uma preparação para a ação principal, os ciberataques começaram cerca de 1 mês antes do exército russo começar a invadir o país: vários grupos, sediados nos EUA e especializados em monitoração de segurança na internet, detectaram tráfegos de dados excessivamente intensos direcionados a servidores (computadores que disponibilizam páginas na internet) localizados na Georgia.

> Semanas antes das bombas começarem a cair na Georgia um pesquisador de segurança trabalhando nos EUA observava um ataque cibernético acontecendo contra aquele país: Jose Nazario da empresa 'Arbor Networks' detectou um intenso fluxo de dados direcionado a [sítios eletrônicos] do governo da Georgia contendo a mensagem "win+love+in+Rusia" ["conquiste+amor+na+rusia"]. Outros especialistas também situados nos EUA afirmam que os ataques virtuais contra a internet na Georgia começaram em 20 de julho, através do envio de várias sequências de dados contendo milhões de requisições [de acesso] - tipo de ataque conhecido como DDoS ['Distributed Denial of Service' ou 'Negação de Serviço Distribuída'] - que sobrecarregaram e efetivamente interromperam o funcionamento de vários servidores na Georgia. (MARKOFF, 2008) [1]

Logo após estes ensaios iniciais começaram os preparativos para os ataques principais que, numa estratégia diversionista, deveriam acontecer de maneira indireta: pessoas ou grupos não identificados, mas claramente alinhadas com os interesses do governo russo naquele momento, criaram dois sítios eletrônicos dedicados a incentivar o repúdio à Georgia. Neles era exibido um manifesto (escrito em russo) contra o país e eram oferecidos gratuitamente programas capazes de prejudicar o funcionamento de páginas na internet e a rede telefônica celular. Junto à seção dedicada aos programas (área de "download") havia uma lista de endereços eletrônicos fornecendo "alvos" cuja operacionalidade era importante para a comunicação do governo da Georgia com o mundo e seus cidadãos. O claro objetivo

1 tradução nossa, do original: "Weeks before bombs started falling on Georgia, a security researcher in suburban Massachusetts was watching an attack against the country in cyberspace. Jose Nazario of Arbor Networks in Lexington noticed a stream of data directed at Georgian government sites containing the message: “win+love+in+Rusia.” Other Internet experts in the United States said the attacks against Georgia’s Internet infrastructure began as early as July 20, with coordinated barrages of millions of requests — known as distributed denial of service, or D.D.O.S., attacks — that overloaded and effectively shut down Georgian servers."

desta estratégia de ação era manter os verdadeiros responsáveis pelo ciberataque o mais ocultos possível ao mesmo tempo em que se estimulava uma grande quantidade de simpatizantes da causa a realizar ataques difusos e não centralizados que, desta maneira, não teriam uma autoria bem definida e seriam muito difíceis de serem controlados e bloqueados pelos computadores (servidores) utilizados pelo governo da Georgia. A página pedia um "esforço especial" nos ataques para uma data determinada.

> O ataque digital contra a Georgia foi coordenado pelo endereços eletrônicos www.stopgeorgia.info (baseado na Alemanha e rapidamente desativado pelo provedor que o mantinha) e www.stopgeorgia.ru. Este último sítio eletrônico era baseado no Reino Unido e foi criado em 9 de agosto de 2008, mantendo-se em operação até o dia 13 de agosto quando o seu serviço foi subitamente interrompido, retornando 24 horas depois sem a seção de software e com um fórum inoperante [...] Na seção de software [enquanto esteve ativa] era possível baixar vários tipos de programas [maliciosos]: um capaz de realizar ataques de sobrecarga de acesso a páginas previamente determinadas (possibilitando assim criar ataques de DDoS ['Negação de Serviço Distribuída' em português]), um programa para tornar o usuário invisível [anônimo] na internet, outro programa para saturação do acesso a internet em redes de celular utilizando VoIP ["Voz sobre IP" em português] e um programa para saturação da linha telefônica celular utilizando a transmissão de SMS [mensagens de texto que fazem parte do protocolo de comunicação de voz em redes celulares]. O sítio pedia que os interessados atacassem uma lista de "alvos" fornecida e conclamava a um esforço especial no dia 13 agosto, declarado o dia de luto pelas vítimas da invasão da Ossétia do Sul [...] (RIOS et al, 2009, p. 36) [2]

O manifesto exibido pelo site se consistia no seguinte texto:

> Nós, os representantes do submundo 'hacker' russo, não iremos tolerar as provocações da Georgia em nenhum dos seus tipos de manifestação. Nós queremos viver num mundo livre, livres de agressões e mentiras no ciberespaço. Nós não precisamos da orientação de autoridades ou de qualquer outra pessoa, agimos de acordo com as nossas convicções baseadas no patriotismo, na consciência e na crença numa justiça forte. Você pode nos chamar de criminosos cibernéticos e terroristas, dizer que estamos começando uma guerra e matando pessoas, mas nós lutaremos e são inaceitáveis as agressões contra a federação russa na internet.
> Nós exigimos o fim dos ataques nos meios digital e físico, e pedimos a todos os meios de comunicação e aos jornalistas que cubram os eventos de maneira objetiva. Até que haja uma mudança na situação atual nós iremos interromper a divulgação de informações falsas oriundas dos governos

2 tradução nossa, do original: "The digital attack to Georgia was coordinated from the domain www.stopgeorgia.info (based in German and quickly closed by the owner of the web server) and www.stopgeorgia.ru. This last site was based on the United Kingdom, created on 9 August of 2008, and kept in operation until 13 August, when it was suspended, return- ing to work after twenty four hours, without the software section and with a inoperative forum [...] On the software section it was possible to download a tool to perform flood attacks with intent to perform an attack by DDoS (Distributed Denial of Service), an anonymization tool, a tool of saturation of telephone lines using a voice over IP software and a tool of mobile phone's saturation using the transmission of SMS (Short Message Service). This website appealed to an attack to a list of targets and called the Internet users to a special effort on the 13th of August, declared day of mourning for the victims of South Ossetia's invasion [...]"

> do ocidente e do governo e mídia da Georgia. Nós chamamos todos aqueles que não são indiferentes às mentiras políticas que a Georgia divulga na internet a contribuir, todos, os que são capazes de impedir a propagação de informações falsas. (RIOS et al, 2009, p. 36) [3]

Não há informações seguras sobre os responsáveis por estes sítios eletrônicos e a origem deste texto (RIOS et al, 2009, p. 41). É interessante então observar no manifesto a preocupação em associar sua autoria a grupos de 'hackers' não devidamente identificados e à filosofia de liberdade na internet, uma liberdade que, entretanto, estaria condicionada ao patriotismo russo e ao repúdio às supostas "agressões" da Georgia e às "informações falsas" divulgadas pela mídia ocidental. O texto demonstra um claro esforço em associar as ideias libertárias da era digital (vide item 2.2, "Idealismo") com a propaganda e ideologia propaladas pelo governo russo.

Entretanto, a ação descentralizada e caótica que seria esperada de uma enorme quantidade de ataques cibernéticos espontâneos deflagrados por inúmeros simpatizantes russos ao redor do mundo não aconteceu. Pelo contrário: diversos tipos de alvos diferentes foram atacados dentro do ciberespaço da Georgia mas, coincidindo perfeitamente com a estratégia militar do governo russo, não houve danos significativos à infraestrutura básica de funcionamento do país (redes de energia, telecomunicações, petróleo, etc). As interrupções causadas foram somente temporárias e concentradas nos sítios eletrônicos dedicados à divulgação de informações e comunicação do governo da Georgia.

> Empresas de comunicação, mídia e transporte foram atacadas na Georgia segundo alguns pesquisadores de segurança. [A empresa] Shadowserver acompanhou o ataque contra contra a Georgia se espalhar através dos computadores do governo do país logo após as tropas russas invadirem a província da Ossétia do Sul. O sítio eletrônico do Banco Nacional da Georgia teve o seu conteúdo adulterado em meio ao ataque. Fotos de ditadores do século XX foram exibidas junto a uma foto do presidente da Georgia na época, Mikheil Saakashvili [...] (MARKOFF, 2008) [4]

3 tradução nossa, do original: "We, the representatives of Russian's hacking underworld, can't tolerate Georgian's provoking, in all their manifestations. We want to live in a free world and free of aggressions and lies in web space. We don't need the orientation of authorities or other people's orientations, but to act in accord with convictions based on patriotism, of conscience and in believing on justice force. You can call us cyber criminals and terrorists, triggering a war and killing people. But we will fight and it's unacceptable the aggression against Russian Federation on internet.
We demand the end of attacks in what regards to field of information and means, and call to all media and journalists to cover the events ob-jectively. Until situation changes, we will stop the divulgation of false information from occidental governments and from Georgian's gov-ernment and media. We appeal to all that aren't indifferent to the lies of websites political Georgian's to contribute, all, who are able to inhibit the propagation of black information."

4 tradução nossa, do original: "In Georgia, media, communications and transportation companies were also attacked, according to security researchers. Shadowserver saw the attack against Georgia spread to computers throughout the government after Russian troops entered the Georgian province of South Ossetia. The National Bank of Georgia's Web site was defaced at one point. Images of 20th-century dictators as well as an image of Georgia's president, Mr. Saakashvili, were placed on the site [...]"

Coerente com a percepção da importância estratégica que a comunicação rápida ocupa no mundo globalizado (vide item 2.3 "O Poder Cibernético na Visão de Nye Jr"), os ciberataques se concentraram no objetivo de debilitar ou anular a capacidade das regiões atacadas e do governo da Georgia como um todo em se comunicar com o mundo externo, de maneira a impedir que informações mais detalhadas sobre o que estava acontecendo fossem divulgadas para a população do país e para o mundo. Citando um estudo específico (BUMGARNER; BORG, 2009) do governo dos EUA, HOLLIS afirma (2011) [5]:

> [...] "Eles não tentaram interromper o funcionamento de sítios eletrônicos que pudessem gerar caos ou danos mais sérios como os ligados à distribuição de energia elétrica ou petróleo, somente aqueles que seriam capazes de causar uma 'perturbação' temporária". "Houve uma decisão política de não atacar diretamente infraestruturas críticas para o país. Entretanto, eles deixaram claro que poderiam tê-lo feito se quisessem; eles mostraram que tinham a capacidade de fazer muito mais" afirma Bumgarner. Este tipo de atitude reproduz com perfeição a estratégia da Rússia contra as instalações que têm uma importância primordial para a Georgia: os oleodutos Baku-Ceyhan, de longe a principal razão pela qual os EUA e o Ocidente como um todo estão interessados na Georgia. Nós já discutimos aqui a maneira como a Rússia realizou bombardeios próximos de toda a extensão do oleoduto sem atingi-lo de fato: uma clara mensagem de que poderiam tê-lo feito se quisessem mas iriam se abster no momento. De fato, o ciberataque se encaixa com perfeição na grande estratégia russa centrada na infraestrutura de transmissão de petróleo da Georgia, conclui Bumgarner.

A sincronia dos ataques cibernéticos com as batalhas travadas pelas forças russas foram notáveis e importantes para a estratégia militar adotada, sugerindo uma atuação da Rússia no Ciberespaço que iria bem além da incitação de terceiros.

> Tanto nos níveis tático quanto operacional localidades geográficas específicas foram visadas dentro do mundo virtual antes que as operações começassem no mundo real. "Muito dos ataques [cibernéticos] mais intensos começaram em sincronia com o início do avanço dos tanques de guerra, apesar das redes já terem sido preparadas com antecedência [os programas maliciosos já estavam prontos para ação muitos dias antes]. E a escolha dos alvos foi particularmente significativa. Os sítios eletrônicos oficiais da cidade de Gori, junto com os sítios das agências locais de notícias, foram desativados antes que os aviões russos chegassem até lá. Como eles sabiam que a cidade de Gori seria bombardeada e não a capital da Georgia ?". "Eu diria, a partir do que eu vi em primeira mão, que houve algum nível de coordenação e/ou direcionamento dos ataques

5 tradução nossa, do original: "[...] they didn't attempt to cripple sites that could have caused chaos or injury, such as those linked to power stations or oil-delivery facilities, but merely those that could trigger comparative "inconvenience." "There was a political decision not to attack those critical infrastructures directly. They made the point that they could launch these attacks. They showed they have the capability to do more," Bumgarner said. This mirrors Russian action against Georgia's paramount strategic installation -- the Baku-Ceyhan oil pipeline, by far the biggest reason why the U.S. and the West as a whole are interested in Georgia. We've discussed here how Russia bombed all around the pipeline without actually hitting it -- a clear message that it could do so if it wished, but would refrain for the moment. Indeed the cyber attack fit into an overall Russian strategy centered on Georgia's oil infrastructure, Bumgarner concludes."

> [por parte do governo russo], especialmente no que se refere à sincronia e os alvos escolhidos." Ao que parece os russos estabeleceram previamente que o governo da Georgia seria o centro das suas operações bélicas, e os ciberataques conduzidos pelas milícias russas deram apoio a estes esforços anulando ou reduzindo a capacidade de comunicação, tanto internamente quanto com o mundo exterior [...] (HOLLIS, 2011) [6]

Os conflitos armados duraram apenas uma semana e as interrupções no Ciberespaço da Georgia foram de grande importância para evitar que o país conseguisse solicitar auxílio internacional a tempo de evitar a derrota perante as forças russas, superiores tanto em termos de armamento quanto em estratégia de ataque.

> [...] A guerra começou oficialmente no dia 7 de agosto de 2008, após crescentes discussões sobre o futuro do território da Ossétia do Sul. As tropas da Georgia iniciaram um ataque militar contra a Ossetia do Sul num grande bombardeio à cidade de Tskhinvali, supostamente em resposta contra uma provocação russa. A Rússia enviou tropas de combate adicionais à Ossétia do Sul e retaliou realizando bombardeios no território da Georgia. A Rússia deslocou forças navais para bloquear o acesso ao território da Georgia e desembarcou a infantaria naval (fuzileiros navais) na costa da Abcássia (próxima à Georgia). O combate terrestre decisivo para a campanha aconteceu com as forças russas e a milícia da Ossétia derrotando as forças militares menos armadas da Georgia na batalha pela cidade de Tskhinvali. A derrota tática nesta frente armada, somada à derrota operacional causada pela invasão russa na parte ocidental do país e a incapacidade de romper ao bloqueio naval imposto, além da dificuldade de fazer com que a sua mensagem fosse ouvida pelo mundo, levou à capitulação da Georgia na guerra. O conflito obrigou cerca de 25.000 cidadãos da Georgia a fugir dos combates em terra como refugiados em deslocamento interno. Os dois países assinaram um acordo de cessar-fogo uma semana depois de iniciada a guerra [...] (HOLLIS, 2011) [7]

6 tradução nossa, do original: "At the tactical and operational levels, specific geographic localities were virtually targeted in cyberspace prior to combat operations in the physical realm. "Many of the most serious attacks began just as the tanks began to roll, although the networks had been set up beforehand. And the choice of targets is especially telling. Official sites in Gori, along with local news sites, were shut down by denial-of-service attacks before the Russian planes got there. "How did they know that they were going to drop bombs on Gori and not the capital?" Jackson asked. "I would say that from what I've seen firsthand, there was at some level actual coordination and/or direction [by the Russian government], especially in regard to the timing and the targets of some of the attacks."" It appears that the Russians selected the Georgian government as the center of gravity to focus its primary attacks upon. Cyberspace domain operations conducted by the Russian cyber militia supported that effort by denying and degrading the Georgian government‟s ability to communicate, both internally and with the outside world [...]"

7 tradução nossa, do original: "[...] The war officially started on 7 August 2008 after several weeks of growing arguments over the future of the South Ossetian territory. Georgian troops initiated a military attack against South Ossetia and began a massive shelling of the town of Tskhinvali in response to alleged Russian provocation. Russia deployed additional combat troops to South Ossetia and retaliated with bombing raids into Georgian territory. Russia deployed naval forces to formally blockade Georgia and landed naval infantry (marines) on Abkhaz coast (near Georgia). The decisive ground combat operation of the campaign resulted in mechanized Russian military and Ossetian militia forces defeating the more lightly armed Georgian military forces in the only large-scale major ground combat of the war (battle for the town of Tskhinvali). Georgian tactical military defeat at the battle of Tskhinvali, operational defeat via Russian uncontested invasion of the western part of Georgia, unchallenged naval blockade of Georgia, and Georgian difficulty getting their media message out to the world, led to Georgia's strategic defeat in the war. The conflict forced approximately 25,000 Georgian residents to flee from ground combat as refugees into internal displacement. The two countries signed a ceasefire agreement a week later [...]"

Observando-se o conflito como um todo se torna difícil admitir que as coincidências muito oportunas entre os ataques físicos e cibernéticos tenham sido obra do acaso. Pelo contrário: o desenrolar dos acontecimentos sugere uma estratégia comum previamente bem definida e levada a cabo com competência e habilidade. A responsabilidade final pelos ciberataques permanece uma incógnita até hoje, mas é inquestionável a importância que eles tiveram no sucesso da operação militar russa.

> Este parece ser o primeiro caso na história de um ataque no domínio cibernético realizado de maneira coordenada com operações de combate nos domínios mais tradicionais de guerra (terra, ar, mar e espaço). "[...] três semanas antes dos bombardeios entre Rússia e Geórgia começarem os ataques virtuais contra os sítios eletrônicos da Geórgia já estavam acontecendo. Desde então os pesquisadores têm tentado descobrir quem foi o grande responsável pelos ataques cibernéticos - unidades militares especializadas em guerra eletrônica, *hackers* patrióticos, bandidos cibernéticos - sem chegar a uma conclusão definitiva. Independente disto "[...] a Rússia invadiu a Geórgia em quatro frentes distintas. Três delas eram convencionais - por terra, ar e mar - enquanto a quarta era nova e envolvia ataques através do ciberespaço [...] É altamente improvável que os ataques simultâneos por terra e Ciberespaço tenham sido coincidência, independente da recusa por parte da Rússia em assumir a responsabilidade pelos atos." O (suposto) ataque cibernético russo sobre as redes militares e governamentais da Geórgia foram um grande sucesso. "Aparentemente 54 sítios eletrônicos relacionados com comunicações, finanças e governabilidade foram atacados por vários focos situados na Rússia [...] de maneira que, ao mesmo tempo em que os tanques e as tropas russas estavam cruzando a fronteira e os bombardeios começavam, os cidadãos da Geórgia não conseguiam acessar as páginas na internet que lhe dariam informações e intruções sobre o que estava acontecendo." As autoridades do país descobriram que o seu acesso à internet e às redes de comunicação eram excepcionalmente vulneráveis à (suposta) interferência russa (HOLLIS, 2011) [8]

8 tradução nossa, do original: "This appears to be the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains (consisting of Land, Air, Sea, and Space). "…three weeks before the shooting war between Georgia and Russia began, online attackers started assaulting Georgia's websites. Since then, researchers have tried to find out who masterminded the network strikes - military electronic warriors, patriotic hackers, cyber-crooks - without finding anything definitive." Nevertheless, "…Russia invaded Georgia on four fronts. Three of them were conventional - on the ground, through the air, and by sea. The fourth was new - their attacks via cyberspace ... It is, quite simply, implausible that the parallel attacks by land and by cyberspace were a coincidence - official denials by Moscow notwithstanding." The (alleged) Russian attack upon the Georgia's military and government networks was highly successful. "It seems that 54 web sites in Georgia related to communications, finance, and the government were attacked by rogue elements within Russia ... So as tanks and troops were crossing the border and bombers were flying sorties, Georgian citizens could not access web sites for information and instructions." Georgian authorities discovered their Internet access and communications networks to be exceptional vulnerable to (alleged) Russian interference."

3.3 Conclusão

Após a fim da URSS e da bipolaridade imposta pelo poder político-econômico socialista como um todo no cenário internacional, o círculo de influência da Rússia sobre os seus ex-Estados-Satélites foi se reduzindo de maneira rápida e drástica. Sob uma análise realista (vide item 2.2b, "Realismo"), isto representa uma ameaça crescente a Moscou devido à intensa redução do seu poder regional tanto em termos militares quanto estratégicos. A geopolítica da Europa Oriental começou a mudar radicalmente com a entrada da Polônia na OTAN em 1998 e, um pouco depois, na reforma de 2004, com a adesão da maior parte dos ex-Estados-Satélites da URSS e de três Estados Bálticos a este tratado de proteção ocidental. Tal qual uma corda que se comprimia ao redor do pescoço russo, a capacidade de defender seus interesses regionais diminuía aceleradamente. A revolução laranja na Ucrânia em 2004 e a consequente alteração na orientação política deste país para um regime simpático ao Ocidente colocou Moscou em estado de alerta com a possibilidade da OTAN chegar às suas fronteiras. O posicionamento de forças militares ocidentais a meros 500 km de distância de Moscou representaria não só uma ameaça definitiva à segurança da Rússia mas também uma influência política poderosa capaz de desestabilizar a federação russa como um todo. Logo depois, a independência do Kosovo em fevereiro de 2008, viabilizada pelo forte apoio da Europa e dos EUA, criando assim mais um país pró-ocidente na região estratégica dos Bálcãs, só fez aumentar o sentimento russo de que o ocidente estava armando um cerco em volta do seu país (FRIEDMAN, 2008).

Diante desta perspectiva altamente desfavorável, era imperativo que a Rússia reagisse e o fizesse num cenário de guerra onde os seus exércitos pudessem realizar uma clara demonstração de força tanto para o Ocidente quanto para os países ainda na sua esfera de influência (FRIEDMAN, 2008).

Os crescentes conflitos étnicos dentro da Georgia, um outro país vizinho à Rússia sob forte influência ocidental, que levaram à insurgência das províncias da Ossétia do Sul e da Abcássia, forneceram aos russos um território muito favorável a estas pretensões, principalmente se considerarmos que os EUA estavam naquele

momento absortos com as guerras no Iraque e no Afeganistão, além de serem obrigados a lidar com a tensão crescente contra o Irã e a desestabilização da situação no Afeganistão. Trata-se então de uma janela de oportunidade para recuperar, de maneira assertiva, um pouco da esfera de influência da antiga União Soviética (FRIEDMAN, 2008).

A ocupação da Ossétia do Sul e o ataque à Georgia se encaixam de maneira muito coerente dentro desta perspectiva. Entretanto, um problema significativo se colocava diante dos russos: como realizar um ataque armado à Georgia, um país em processo de se tornar membro da OTAN, sem que a Europa ou os próprios EUA intervenham enviando auxílio militar ou até mesmo tropas ? Uma resposta possível estaria na utilização do tempo como um aliado, ou seja, a elaboração de uma campanha rápida e altamente eficaz capaz de fazer o inimigo sucumbir antes que o Ocidente tivesse tempo de esboçar alguma reação; ao mesmo tempo em que manteria resguardados os interesses ocidentais nesta região, evitando causar maiores danos à infraestrutura da Georgia e, principalmente, mantendo ileso o oleoduto de Baku-Tbilisi-Ceyhan, o grande estímulo para a existência de apoio externo àquele país. Para os russos, o grande objetivo da campanha militar seria garantir sua esfera de influência na Ossétia do Sul, evitando que a Georgia retome este território, e realizar um grande demonstração de força que não deixe dúvidas ao Ocidente e seus aliados que a Rússia é uma potência militar moderna e altamente competente. É neste último aspecto que o ataque cibernético ganha importância.

Em termos comparativos a Georgia é um país ainda incipiente no uso do Ciberespaço. Em 2009, logo após o término do conflito em questão, somente cerca de 22% da população do país fazia uso regular da internet, e em 2015 ainda não havia uma movimentação comercial em meio digital que pudesse ser comparada com a dos países mais desenvolvidos (Internet World Stats, 2017). Segundo uma empresa especializada, a importância do Ciberespaço para a Georgia em 2008 era menor do que para vários países com baixo índice de desenvolvimento.

> [A Georgia] ocupa 74ª posição numa lista de 234 países em termos de quantidade de endereços na internet, atrás da Nigéria, Bangladesh, Bolívia e El Salvador, afirma a empresa Renesys, especializada em fornecer dados sobre a internet. Os ciberataques têm um impacto muito menor neste país do que numa nação mais dependente de conexões digitais como Israel, Estonia ou EUA, onde serviços vitais à população como transporte, energia elétrica e transações bancárias são controlados via internet. (MARKOFF, 2008) [1]

Entretanto, mesmo com uso reduzido da comunicação digital em rede o país sofreu graves limitações devido à simultaneidade das ações militares tradicionais (terrestres, aéreas e navais) com os ataques cibernéticos. A guerra entre a Rússia e a Georgia em 2008 é considerada o primeiro grande conflito armado onde o domínio cibernético foi utilizado como uma arma efetiva junto aos domínios convencionais de ação militar (Hollis, 2011).

A demonstração russa de extrema habilidade no domínio cibernético, apresentando-se ao mundo desta forma como uma força moderna e competente, é, mais uma vez do ponto de vista realista, uma das grandes vitórias desta guerra perante o Ocidente, principalmente perante os EUA e Israel, países que detém um notório poder, tanto ofensivo quanto defensivo, neste novo domínio bélico (vide capítulo 4, "Stuxnet"). Sob esta perspectiva o ciberataque russo foi primoroso: conseguiu ocultar com eficiência os seus verdadeiros perpetradores, conseguiu debilitar seriamente a capacidade de reação e divulgação dos acontecimentos por parte do governo da Georgia, demonstrou um alto controle técnico ao evitar danos maiores (interrupção de sistemas de fornecimento de eletricidade, petróleo, etc) e, atuando junto com os ataques físicos, anulou completamente a capacidade de reação da Georgia fazendo com que o país capitulasse em apenas cinco dias de combates.

Analisando o mesmo conflito agora sob o ponto de vista neoliberal (vide item 2.2c, "Neoliberalismo") é possível chegar a conclusões semelhantes. Considerando-se que cerca de 60% da exportação russa está diretamente apoiada em petróleo bruto (IMF, 2017) e seus principais compradores são a Europa e EUA (OEC, 2017), considerando também que grande parte das importações da Rússia (aproximadamente 50%) provém da Europa (OEC, 2017), percebe-se que há amplas trocas comerciais entre a economia russa e o Ocidente, o que inibiria agressões militares entre ambos devido ao estabelecimento de uma relação de interdependência complexa. Por outro lado, entre a Rússia e a Georgia as relações comerciais eram insignificantes para o lado russo em 2008 (BIRNBAUM, 2015) e o país representava, devido ao oleoduto de Baku-Tbilisi-Ceyhan, majoritariamente um grande inimigo comercial (MOUAWAD, 2008). Desta forma, faz sentido que a Rússia admita um ataque armado ao território do país vizinho buscando reduzir a sua

autonomia política e comercial, ao mesmo tempo em que tenta evitar um conflito direto com o Ocidente. Segundo a visão de NYE JR para o poder cibernético (vide item 2.3, "O Poder Cibernético na Visão de Nye Jr"), o esforço da campanha cibernética contra a Georgia poderia ser entendido como uma ação visando restringir a presença da Georgia no Ciberespaço e, desta forma, ocultar informações, reduzindo assim a possibilidade de intervenções inimigas, seja pelo poder "suave" ("soft power": propaganda antirússia na mídia ocidental, campanhas de grupos pacifistas, resoluções da ONU, etc), seja pelo "rígido" ("hard power": retaliações ou auxílio cibernético por parte de simpatizantes ou de países do Ocidente, sanções econômicas, etc). Ao debilitar a capacidade de comunicação da Georgia com o mundo através da internet, a Rússia fez com que este país, mesmo com um nível ainda incipiente de atividade digital, retrocedesse varias décadas em termos de capacidade de mobilização e interação interna e externa, e conseguiu que ele fosse temporariamente alijado da comunidade internacional, uma vez que se tornou muito difícil obter notícias confiáveis sobre o desenrolar da guerra e o que estaria efetivamente acontecendo em seu território.

Excluída do Ciberespaço, a Georgia perdeu a capacidade de lutar a principal batalha que caracteriza o cenário internacional moderno: a batalha das informações.

CAPÍTULO IV

ESTUDO DE CASO: STUXNET

4.1 Antecedentes

O Irã deu os seus primeiros passos na tecnologia atômica durante a década de 1950 com a adesão pelo então monarca deste país, o Xá Mohammad Reza Pahlavi, ao programa internacional chamado "Átomos para a Paz". Este projeto, criado pelos EUA durante a administração do presidente Dwight D. Eisenhower, tinha como objetivo incentivar o uso civil e pacífico da energia atômica oferecendo aos seus aliados o auxílio necessário para a construção de usinas elétricas nucleares. Alguns anos depois, mantendo-se nesta mesma tendência, a administração de Pahlavi assina o Tratado Internacional de Não Proliferação Nuclear (TNP) em 1968, tornando-se o 51º país do mundo a se comprometer em não utilizar a tecnologia nuclear para fins militares (SINHA; BEACHY, 2015).

> O Irã mantém, já há quase 50 anos, um programa nuclear que começou com a compra de um reator nuclear estadunidense em 1959. Na época, os planos do Xá para construir 23 usinas de energia nucleares até os anos 1990 foram considerados grandiosos mas não chegaram a ser vistos como uma intenção não declarada de empreender o desenvolvimento de armas nucleares. E o motivo disto é o fato de que o Irã não se interessou por tecnologias de enriquecimento ou reprocessamento do combustível nuclear [essenciais para a construção deste tipo de armamento]. Algumas suspeitas neste sentido surgiram ao longo do tempo mas foram afastadas no período entre a revolução iraniana de 1979 e o fim da guerra Irã-Iraque, quando todas as atividades nucleares iranianas foram interrompidas.
> (SQUASSONI, 2006, p. 1) [1]

O fim do regime de Pahlavi, em 1979, trouxe uma forte mudança na orientação política do país agora sob controle de um governo revolucionário teocrático com forte tendência antiamericanista. O novo líder do país e também autoridade máxima religiosa, o Aiatolá Rudollah Khomeini, declara-se contra o uso da energia nuclear e com isso vários dos especialistas desta área fogem do país temendo a perseguição da polícia política ao mesmo tempo em que o acordo de cooperação com o EUA é abandonado. Entretanto, esta política de desprezo pela tecnologia nuclear começa a mudar no final dos anos 1980 quando um especialista paquistanês, Abdul Qadeer Khan, responsável pelo desenvolvimento do programa nuclear no Paquistão, vende para o Irã, Coréia do Norte e Líbia várias informações secretas sobre enriquecimento de urânio, informações estas que poderiam levar à construção de

[1]tradução nossa, do original: "Iran has had a nuclear program for close to 50 years, beginning with a research reactor purchased from the United States in 1959. The Shah's plan to build 23 nuclear power reactors by the 1990s was regarded as grandiose, but not necessarily viewed as a "back door" to a nuclear weapons program, possibly because Iran did not then seek the technologies to enrich or reprocess its own fuel. There were a few suspicions of a nuclear weapons program, but these abated in the decade between the Iranian 1979 revolution and the end of the Iran-Iraq war, both of which brought a halt to nuclear activities."

uma bomba atômica. O novo líder supremo do país, Aiatolá Ali Khamenei, sucessor de Khomeini, assume o poder em 1989 e decide retomar o programa de desenvolvimento nuclear. Em 1995 o Irã anuncia um acordo com a Rússia para finalizar a construção de uma usina elétrica nuclear na província de Bushehr (SINHA; BEACHY, 2015).

Suspeitando de que o Irã estava empreendendo pesquisas secretas visando a construção de armas nucleares, os EUA impõem as primeiras sanções econômicas em 1996, impedindo diversas empresas nacionais e estrangeiras de negociarem ou investirem no país liderado por Khamenei. Em 2002 as suspeitas são confirmadas quando um grupo de dissidentes iranianos divulga documentos provando a existência de uma grande usina de enriquecimento clandestina na localidade de Natanz, e de um reator de água pesada na cidade de Arak. Os EUA imediatamente acusam o Irã de desenvolver armas de destruição em massa e esta denúncia inicia uma série de incidentes envolvendo violações sucessivas por parte do Irã aos acordos assumidos previamente em diversas negociações internacionais. As relações do mundo ocidental com o país persa se degeneram a tal ponto que, em 2008, o Conselho de Segurança da ONU autoriza a primeira lista de sanções econômicas mundiais, banindo completamente a entrada no Irã de matéria prima ou tecnologia associada com o enriquecimento de urânio e construção de mísseis balísticos (SINHA; BEACHY, 2015).

> Em 2002, o Conselho Nacional de Resistência do Irã ajudou a revelar atividades iranianas de pesquisa atômica não declaradas ao fornecer informações sobre as instalações nucleares de Natanz (enriquecimento de Urânio) e Arak (produção de água pesada). Três anos de intensas inspeções por parte da IAEA (International Atomic Energy Agency - Agência Internacional de Energia Atômica -) já haviam demonstrado os esforços secretos por parte do Irã para conseguir enriquecer urânio (desenvolvimento de tecnologias como centrífugas, vaporização atômica por LASER e separação de isótopos através de LASER molecular) além de tentativas de realizar a separação do plutônio, incluindo a existência de material importado não declarado. As autoridades iranianas atrasaram as inspeções, alteraram as explicações para as discrepâncias encontradas, esvaziaram instalações e, em um caso, Lavizan-Shian, chegaram a destruir completamente uma usina existente. Segundo o diretor geral da IAEA, General Mohamed ElBaradei, "O Irã tentou encobrir muitas das suas atividades de pesquisa com energia atômica, e eles aprenderam a fazê-lo da maneira mais difícil" (SQUASSONI, 2006, p. 2) [2]

[2]tradução nossa, do original: "In 2002, the National Council of Resistance of Iran (NCR) helped expose Iran's undeclared nuclear activities by providing information about nuclear sites at Natanz (uranium enrichment) and Arak (heavy water production). Three years of intensive inspections by the IAEA revealed significant undeclared Iranian efforts in uranium enrichment (including centrifuge, atomic vapor laser and molecular laser isotope separation techniques) and separation of plutonium, as well as undeclared imported material. Iranian officials have delayed inspections, changed explanations for discrepancies, cleaned up facilities and in one case, Lavizan-Shian, razed a site. According to IAEA Director General Mohamed ElBaradei, 'Iran tried to cover up many of their activities, and they learned the hard way.'"

Afirma Sanger (2009) que, preocupado com a possibilidade de ter um antagonista regional armado com a bomba atômica, Israel solicita secretamente aos EUA que lhe forneçam mísseis especiais recém-desenvolvidos que seriam capazes de destruir as instalações subterrâneas iranianas, de maneira a conduzir um ataque aéreo surpresa ao país persa e anular as suas ambições nucleares. Entretanto, temendo que uma agressão deste porte leve a uma radicalização ainda maior do regime de Khamenei, e sofrendo um grande desgaste político interno devido à guerra do Iraque, o então presidente dos EUA, George W Bush, recusa a solicitação mas concorda em iniciar um programa de sabotagem cibernético.

4.2 Um novo tipo de arma cibernética

O programa de computador vulgarmente conhecido como 'vírus' é um tipo específico de software que, tal qual o seu equivalente biológico, é capaz de fazer cópias de si mesmo e se espalhar por vários computadores com o objetivo de agir de maneira oculta, realizando operações diversas sem que os responsáveis pelos sistemas 'infectados' saibam o que está acontecendo (STALLINGS, 2012, p. 182). A análise realizada sobre o código do 'vírus' que contaminou as instalações atômicas iranianas deixou claro que ele foi criado especialmente para atuar sobre o equipamento utilizado por elas além de apresentar um comportamento inédito até então: ele modificava o funcionamento dos sistemas computadorizados que controlam as centrífugas de maneira a fazê-las girar rápido demais e causar danos físicos a estes equipamentos. Ou seja: assumindo um comportamento totalmente diferente dos códigos maliciosos vistos até então (que se restrigiam a danificar as informações armazenadas e nunca o equipamento que as armazena), este programa vai bem além e causa danos aos dispositivos físicos conectados ao computador, algo totalmente novo naquela época (FLEMING, 2010).

> O stuxnet, nome pelo qual este programa passou a ser conhecido, era diferente de qualquer outra praga virtual criada até o momento. Ao invés de assumir o controle dos computadores-alvo e roubar informações deles, ele invadiu o reino digital com o objetivo de causar danos aos equipamentos externos controlados pelos computadores ['infectados']. (ZETTER, 2014) [3]

[3]tradução nossa, do original: "Stuxnet, as it came to be known, was unlike any other virus or worm that came before. Rather than simply hijacking targeted computers or stealing information from them, it escaped the digital realm to wreak physical destruction on equipment the computers controlled."

Segundo Mueller e Yadegari (2012) o "stuxnet é um verme digital sofisticado e desenvolvido para atacar especificamente sistemas SCADA (dedicados ao controle de instalações industriais) da empresa Siemens"[4] A grande complexidade do seu código e a enorme quantidade de trabalho necessária para desenvolvê-lo sugere não só a atuação de equipes altamente qualificadas de programação como também o acesso a detalhes muito específicos de funcionamento dos sistemas de controle industriais instalados pelo governo iraniano em Natanz, as instalações secretas descobertas em 2002 e dedicadas ao enriquecimento de urânio.

> Ele faz uso de quatro vulnerabilidades do tipo 'dia zero' (vulnerabilidades de segurança existentes num programa mas ainda desconhecidas pelos seus programadores responsáveis), utiliza 'rootkits' (técnicas avançadas para se ocultar dos usuários e dos programas antivírus) efetivos tanto em Windows quanto nos seus computadores-alvo, e ainda possui dois certificados digitais roubados para autorizar a sua execução [junto aos computadores 'infectados']; seus criadores necessitavam de uma enorme quantidade de conhecimento sobre os seus sistemas-alvo [para desenvolver um programa deste tipo] [...] (MUELLER; YADEGARI, 2012) [5]

Segundo Bradley (2016), as vulnerabilidades chamadas de 'dia zero' são as mais valorizadas entre os desenvolvedores de códigos maliciosos (*hackers*) e, por isso, quando descobertas são vendidas por um preço altíssimo nos seus respectivos mercados negros, ao mesmo tempo em que é feito um enorme esforço para manter o seu conteúdo em segredo. Encontrar um vírus de computador que utilize uma vulnerabilidade deste tipo é bem difícil (embora aconteça uma vez ou outra), já encontrar algum vírus que faça uso de quatro (ainda mais voltadas para um sistema altamente específico) se trata de um caso tão inédito que configura mais uma evidência a favor da suspeita de que o stuxnet foi desenvolvido por equipes muito bem qualificadas e financiadas.

Mais ainda, o vírus teve várias versões que cresceram em complexidade e eficiência, sempre voltadas para a alteração perniciosa do funcionamento de centrífugas em sistemas exatamente do tipo em uso pelos iranianos em Natanz.

> O stuxnet trabalhou silenciosamente na sabotagem das centrífugas em Natanz por cerca de um ano. Uma versão anterior do vírus manipulava as válvulas que aumentavam a pressão dentro das centrífugas danificando os aparelhos e prejudicando o processo de enriquecimento. As centrífugas são

[4]tradução nossa, do original: "Stuxnet is a sophisticated worm designed to target only specific Siemens SCADA (industrial control) systems"

[5]tradução nossa, do original: "It makes use of an unprecedented four 0-day vulnerabilities- attacks that make use of a security vulnerability in an application, before the vulnerability is known to the application's developers. It also uses rootkits - advanced techniques to hide itself from users and anti-malware software - on both Windows and the control computers it targets. It employs two stolen digital certificates to sign its drivers, and its creators needed a large amount of knowledge of its targeted systems."

> grandes tubos cilíndricos que - conectados por canos numa configuração de funcionamento chamada 'cascata' - giram em velocidade supersônica para separar os isótopos de urânio contidos num composto gasoso, de maneira a produzir combustível para usinas nucleares de energia elétrica e [num nível bem mais alto de pureza] para armas nucleares. No momento dos ataques cada 'cascata' alocada em Natanz possuía 164 centrífugas. O gás de urânio fluía através dos canos para as centrífugas em estágios, tornando-se cada vez mais 'enriquecido' [maior nível de pureza] ao passar por cada um deles [...] (ZETTER, 2014) [6]

As versões mais avançadas do stuxnet alteravam não só a pressão das válvulas mas também a velocidade de rotação das centrífugas, fazendo com que o processo de enriquecimento (obtenção de combustível nuclear de maior pureza) fosse definitivamente inutilizado e chegando até mesmo a causar a destruição do equipamento, nos momentos em que rotação atingia valores acima da velocidade máxima suportada. Tudo isso enquanto o sistema de controle indicava funcionamento normal das centrífugas. Estas ocorrências foram testemunhadas por profissionais da agência internacional de energia atômica durante uma visita de inspeção.

> Em janeiro de 2010, os inspetores da Agência Internacional de Energia Atômica, durante uma visita à usina de enriquecimento de Natanz, notaram que as centrífugas estavam apresentando um comportamento errático de maneira nunca vista antes. A causa era um completo mistério e, aparentemente, a mesma dúvida afligia os técnicos iranianos que tentavam substituir as centrífugas enquanto os inspetores os observavam (ZETTER, 2014) [7]

Não há informações precisas mas estima-se que o stuxnet tenha causado um dano significativo às operações de enriquecimento em Natanz e, embora não tenha sido capaz de paralizar completamente o funcionamento das instalações, a sua ação deve ter atrasado bastante o programa nuclear iraniano.

> [...] Assumindo que o stuxnet tinha a intenção de prejudicar o funcionamento do programa de desenvolvimento de armas nucleares iraniano, podemos dizer que ele realizou um bom trabalho: é possível que tenha destruído 1000 centrífugas em Natanz, cerca de 11% do total instalado naquela

[6]tradução nossa, do original: "Stuxnet has already been at work silently sabotaging centrifuges at the Natanz plant for about a year. An early version of the attack weapon manipulated valves on the centrifuges to increase the pressure inside them and damage the devices as well as the enrichment process. Centrifuges are large cylindrical tubes—connected by pipes in a configuration known as a “cascade”—that spin at supersonic speed to separate isotopes in uranium gas for use in nuclear power plants and weapons. At the time of the attacks, each cascade at Natanz held 164 centrifuges. Uranium gas flows through the pipes into the centrifuges in a series of stages, becoming further “enriched” at each stage [...]"

[7]tradução nossa, do original: "in january 2010, inspectors with the International Atomic Energy Agency visiting the Natanz uranium enrichment plant in Iran noticed that centrifuges used to enrich uranium gas were failing at an unprecedented rate. The cause was a complete mystery—apparently as much to the Iranian technicians replacing the centrifuges as to the inspectors observing them."

> época. Considerando-se que o Irã não possui uma quantidade ilimitada de centrífugas, e as que ele possui costumam falhar com certa frequência, trata-se de um decréscimo significativo, embora não com consequências fatais para o programa. O stuxnet atrasou a produção de urânio enriquecido e é muito provável que tenha semeado o caos entre os responsáveis pelo projeto (MUELLER; YADEGARI, 2012) [8]

4.3 O Ataque

Segundo Sanger (2012), os esforços de desenvolvimento do stuxnet começaram no governo Bush e continuaram durante o início do governo Obama, quando o vírus de computador acidentalmente se espalhou pelo mundo e, por isso, acabou sendo descoberto.

O projeto secreto de desenvolvimento foi batizado do "jogos olímpicos" e começou devido à falta de opções de Bush para lidar com a ameaça iraniana.

> O esforço para desenvolver o projeto 'jogos olímpicos' começou em 2006 quanto o presidente George W. Bush tinha muito poucas opções para lidar com o Irã. Naquela época os aliados europeus estavam divididos sobre os custos que a imposição de sanções contra Teerã teria sobre as suas próprias economias. Além disso, depois de ter mentido sobre o suposto programa nuclear iraquiano [para ajudar a justificar a invasão àquele país], Bush tinha pouca credibilidade internacional para discutir as ambições nucleares de outros países. Os iranianos pareciam perceber esta vulnerabilidade e, frustrados nas tentativas de negociação, retomaram o enriquecimento de urânio numa instalação subterrânea em Natanz, instalação esta cuja existência havia sido descoberta há apenas 3 anos atrás. (SANGER, 2012) [9]

Inicialmente a ideia era criar um vírus que trabalhasse silenciosamente apenas enviando dados sobre o funcionamento do sistema, de maneira que a estrutura elétrica e eletrônica das instalações em Natanz fossem conhecidas a fundo antes de se tentar danificar as centrífugas de alguma maneira. Este primeiro estágio do trabalho foi chamado de *beacon* (farol).

[8]tradução nossa, do original: "Assuming that Stuxnet was intended to damage this suspected nuclear weapons program, it was somewhat effective: it may have destroyed 1,000 centrifuges at Natanz, about 11% of the total number installed at the time. Also, Iran doesn't have an unlimited number of centrifuges, and the ones they do have tend to fail relatively often, so such a decrease is significant, albeit not immediately fatal to the program. In addition, Stuxnet decreased production of enriched uranium and likely sowed chaos within the Iranian nuclear program."

[9]tradução nossa, do original: "The impetus for Olympic Games dates from 2006, when President George W. Bush saw few good options in dealing with Iran. At the time, America's European allies were divided about the cost that imposing sanctions on Iran would have on their own economies. Having falsely accused Saddam Hussein of reconstituting his nuclear program in Iraq, Mr. Bush had little credibility in publicly discussing another nation's nuclear ambitions. The Iranians seemed to sense his vulnerability, and, frustrated by negotiations, they resumed enriching uranium at an underground site at Natanz, one whose existence had been exposed just three years before."

> O primeiro estágio dos trabalhos era desenvolver um código de computador que pudesse se inserido no sistema de controle, que tinha sido construído pela empresa alemã Siemens e um fabricante iraniano, para mapear o seu funcionamento. A ideia era obter o equivalente a um diagrama elétrico das instalações de Natanz para compreender como os computadores faziam para controlar centrífugas gigantes girando a velocidades altíssimas. As conexões deste sistema eram complexas e, a não ser que cada circuito fosse bem compreendido nos seus detalhes, qualquer esforço para controlá-lo poderia ser mal sucedido. (SANGER, 2012) [10]

O grande problema era que o vírus precisava enviar as informações de volta para a NSA através da internet e isto nunca aconteceria dentro de Natanz, já que as instalações eram subterrâneas e funcionavam completamente isoladas do mundo exterior. Qualquer tentativa neste sentido dependeria totalmente de agentes infiltrados ou erros de segurança dos técnicos envolvidos na manutenção dos equipamentos. Segundo um dos participantes o presidente Bush "estava cético [quando as possibilidades de sucesso] mas, na falta de outras opções, autorizou o início do projeto." [11] (SANGER, 2012)

Só que, algum tempo depois, as pequenas expectativas iniciais sofreram uma significativa melhoria com a entrada no projeto de especialistas israelenses. Os EUA viam grandes vantagens no envolvimento de Israel, não só pelo enorme interesse deste país em sabotar as planos iranianos, mas principalmente pelo fato de que esta seria a melhor maneira de dissuadi-los dos seus planos de bombardear o Irã.

> A colaboração intensa e incomum com Israel foi estimulada por dois imperativos: a unidade 8200, parte das forças militares israelenses, tinha um conhecimento técnico que rivalizava com o da NSA e, além disso, possuía informações detalhadas sobre as operações em Natanz, o que era vital para que o ciberataque fosse bem sucedido. Mas as autoridades estadunidenses também tinham um outro interesse: convencer os israelenses a desistir do ataque preemptivo contra as instalações nucleares iranianas. Para isso era necessário mostrá-los que esta nova linha de ataque seria bem sucedida. E a única maneira de convencê-los disto, diversas autoridades [dos EUA] confirmaram nas entrevistas, era fazer com que os israelenses estivessem profundamente envolvidos em cada aspecto do programa (SANGER, 2012) [12]

[10]tradução nossa, do original: "The first stage in the effort was to develop a bit of computer code called a beacon that could be inserted into the computers, which were made by the German company Siemens and an Iranian manufacturer, to map their operations. The idea was to draw the equivalent of an electrical blueprint of the Natanz plant, to understand how the computers control the giant silvery centrifuges that spin at tremendous speeds. The connections were complex, and unless every circuit was understood, efforts to seize control of the centrifuges could fail."

[11]tradução nossa, do original: "[...] Mr. Bush was skeptical, but lacking other options, he authorized the effort."

[12]tradução nossa, do original: "The unusually tight collaboration with Israel was driven by two imperatives. Israel's Unit 8200, a part of its military, had technical expertise that rivaled the N.S.A.'s, and the Israelis had deep intelligence about operations at Natanz that would be vital to making the cyberattack a success. But American officials had another interest, to dissuade the Israelis from carrying out their own pre-emptive strike against the Iranian nuclear facilities. To do that, the Israelis would have to be convinced that the new line of attack was working. The only way to convince them, several officials said in interviews, was to have them deeply involved in every aspect of the program."

Não demorou para que os dois países desenvolvessem um programa de computador grande e complexo chamado "the bug" (o erro), capaz de invadir e manipular secretamente os sistemas iranianos. Mas, antes de ser colocado em ação, ele precisava ser testado, e para isso os EUA construíram, sob intenso segredo, algumas réplicas das centrífugas iranianas e do seu sistema de controle. O modelo básico utilizado pelo Irã tinha sido comprado de Abdul Qadeer Khan, o especialista paquistanês que vendeu informações secretas sobre técnica de enriquecimento de urânio no mercado negro internacional. O trabalho de construção das réplicas foi então facilitado pelo fato de que os EUA já haviam apreendido algumas centrífugas deste tipo na Líbia, também vendidas por Khan para o ditador Muammar el-Qaddafi (SANGER, 2012).

Estes testes foram surpreendentemente bem sucedidos: o stuxnet conseguiu invadir os computadores e se manter escondido por várias semanas antes de começar a acelerar excessivamente as centrífugas, causando a destruição delas. Para os participantes do programa ficou claro neste momento que a primeira bomba cibernética havia sido contruída. Afirmou Michael V. Hayden, ex-chefe da CIA, sem fornecer maiores informações sobre o incidente: "[...] este é o primeiro ataque em grande escala no qual uma arma cibernética é utilizada para realizar destruição física [...]" (SANGER, 2012) [13]

Mas o desafio estava apenas começando. Como a instalação de Natanz é totalmente isolada do mundo exterior, ainda faltava encontrar uma maneira de inserir o código nas máquinas.

> Colocar o vírus dentro de Natanz não seria uma tarefa fácil. Os EUA e Israel iriam depender de engenheiros, técnicos de manutenção e outros - tanto espiões quanto colaboradores involuntários - com acesso físico às instalações. Este é nosso "pulo do gato", afirmou um dos arquitetos do plano: sempre há um idiota que não dá a devida atenção à segurança com um pendrive na mão (SANGER, 2012) [14]

Ao final de algum tempo, utilizando pendrives previamente preparados e estratégias como a infecção de computadores das empresas fornecedoras de matéria-prima para Natanz, o vírus finalmente alcançou o seu destino e começou a

[13]tradução nossa, do original: "This is the first attack of a major nature in which a cyberattack was used to effect physical destruction [...]"

[14]tradução nossa, do original: "Getting the worm into Natanz, however, was no easy trick. The United States and Israel would have to rely on engineers, maintenance workers and others — both spies and unwitting accomplices — with physical access to the plant. “That was our holy grail,” one of the architects of the plan said. “It turns out there is always an idiot around who doesn’t think much about the thumb drive in their hand.”"

causar prejuízos em 2008. À princípio, segundo comunicações interceptadas pelo serviço secreto estadunidense (e posteriormente reveladas por um dos participantes do programa) os iranianos ficaram totalmente confusos e não conseguiram entender a origem dos problemas: pensavam que eram causados por peças defeituosas, erros de projeto ou incompetência pura e simplesmente (ZETTER, 2014).

> Os iranianos ficaram confusos em parte porque os ataques empreendidos pelo vírus nunca eram iguais. Além disso, o código se mantinha totalmente quieto por várias semanas, escondido dentro do sistema, e quando atacava enviava informações para a sala de controle indicando funcionamento normal da centrífuga. Segundo comentou uma autoridade estadunidense "esta deve ter sido a parte mais brilhante do código" (SANGER, 2012) [15]

As informações recebidas pelo serviço secreto estadunidense indicavam que falhas conseguiram causar grandes problemas para as equipes envolvidas no projeto nuclear iraniano. Toda a vez que o mal funcionamento começava as equipes de controle desligavam todo o grupo de 164 centrífugas, temendo alguma operação de sabotagem. Descobriu-se que vários funcionários foram despedidos e alguns dos responsáveis punidos, sem que se descobrisse o real motivo dos problemas que continuavam a acontecer aparentemente de maneira aleatória (ZETTER, 2014).

> Entre junho e agosto [de 2009] o número de centrífugas enriquecendo urânio em Natanz começou a cair. Não está claro se isto foi causado pela nova versão do stuxnet ou ainda era efeito da versão anterior mas, de uma forma ou de outra, apenas 4.592 centrífugas estavam funcionando, um decréscimo de 328 desde junho. Em novembro o total caiu ainda mais para 3.936, uma diferença de 984 em 5 meses. Mais ainda, embora novas centrífugas tenham sido instaladas, nenhuma delas estava sendo alimentada (ZETTER, 2014) [16]

O início do governo de Barack Obama correspondeu ao que parece ter sido o momento de maior sucesso da operação. Determinado em evitar que o Irã conseguisse a bomba atômica sem que fosse necessário empreender um ataque armado, Obama não poupou esforços ao projeto "Jogos Olímpicos".

[15]tradução nossa, do original: "The Iranians were confused partly because no two attacks were exactly alike. Moreover, the code would lurk inside the plant for weeks, recording normal operations; when it attacked, it sent signals to the Natanz control room indicating that everything downstairs was operating normally. “This may have been the most brilliant part of the code,” one American official said."

[16]tradução nossa, do original: "[...] between June and August the number of centrifuges enriching uranium gas at Natanz began to drop. Whether this was the result solely of the new version of Stuxnet or the lingering effects of the previous version is unknown. But by August that year, only 4,592 centrifuges were enriching at the plant, a decrease of 328 centrifuges since June. By November, that number had dropped even further to 3,936, a difference of 984 in five months. What’s more, although new machines were still being installed, none of them were being fed gas."

> "Desde os seus primeiros dias na presidência ele estava totalmente comprometido em atrasar o programa nuclear iraniano, acompanhando pessoalmente cada passo das iniciativas tomadas, sejam elas diplomáticas, seja a implementação das sanções ou as principais decisões relacionadas" comentou um alto funcionário do governo Obama (SANGER, 2012) [17]

> Os responsáveis pelo projeto "Jogos Olímpicos" o encontravam na "sala de crise" e costumavam levar o que chamavam de "cobertor de cavalo", um diagrama esquemático gigante e dobrável exibindo as instalações nucleares iranianas. Obama autorizava a continuidade dos ataques e, com intervalo de algumas semanas - mas sempre após um ataque mais importante - tomava conhecimento dos acontecimentos e autorizava os próximos passos. Algumas vezes trata-se de um golpe mais arriscado e ousado do que o outro realizado anteriormente (SANGER, 2012) [18]

O stuxnet foi criado para agir sobre um ambiente bem específico e definido, de maneira que o seu código verificava se o Sistema Operacional e as conexões do mesmo correspondiam ao alvo desejado antes de começar a se replicar. Um erro cometido numa das revisões comprometeu esta verificação e fez com que o stuxnet começasse a se espalhar por outros sistemas. No momento em que um dos engenheiros nucleares iranianos conectou à internet o seu computador portátil utilizado em Natanz, o stuxnet começou a se espalhar pelo mundo tal qual um vírus comum. E embora ele não causasse danos aos computadores pessoais (não havia centrífugas nem sistemas SCADA Siemens conectados a eles) a sua presença começou a ser notada pelos especialistas no combate às pragas virtuais até que o código do vírus e suas inúmeras peculiaridades começou a ser conhecido e divulgado.

> Um erro no código, eles disseram, levou o stuxnet a se espalhar a partir do computador portátil de um dos engenheiros, enquanto estava conectado às centrífugas. Ao sair de Natanz e acessar a internet o engenheiro, sem saber, começou a replicar o stuxnet pelo mundo afora. O código americano-israelense falhou em reconhecer a mudança no ambiente dentro do qual ele estava operando [e começou a funcionar como um vírus comum]. De repente, o stuxnet estava exposto na internet, apesar das suas intenções não serem claras aos usuários comuns (SANGER, 2012) [19]

[17]tradução nossa, do original: " “From his first days in office, he was deep into every step in slowing the Iranian program — the diplomacy, the sanctions, every major decision,” a senior administration official said"

[18]tradução nossa, do original: "The architects of Olympic Games would meet him in the Situation Room, often with what they called the “horse blanket,” a giant foldout schematic diagram of Iran’s nuclear production facilities. Mr. Obama authorized the attacks to continue, and every few weeks — certainly after a major attack — he would get updates and authorize the next step. Sometimes it was a strike riskier and bolder than what had been tried previously."

[19]tradução nossa, do original: "An error in the code, they said, had led it to spread to an engineer’s computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed. It began replicating itself all around the world. Suddenly, the code was exposed, though its intent would not be clear, at least to ordinary computer users."

Em 2010, cerca de 2 anos após ter iniciado as suas operações de sabotagem industrial, o stuxnet começou a se tornar conhecido através das empresas fabricantes de softwares antivírus e artigos de especialistas divulgados na internet. Entretanto, mesmo com o risco dos ataques secretos serem revelados a qualquer momento, Obama não desistiu da operação. As negociações para conseguir o recrudescimento das sanções econômicas contra o Irã ainda estavam em andamento (seriam implementadas somente em 2011) e a ameaça de Israel bombardear as instalações iranianas ainda pairava sobre o cenário internacional. Segundo fontes próximas ao governo estadunidense da época, ao ser questionado sobre o vazamento do código do stuxnet para a internet Obama respondeu com uma evasiva e mandou a operação continuar.

> "Não acredito que tenhamos informações suficientes [sobre as implicações deste vazamento]" disse Obama ao grupo naquele dia, segundo fontes próximas. E, enquanto isso, ele ordenou que os ataques continuassem. Eles eram a melhor esperança de interromper o programa nuclear iraniano até que as sanções econômicas entrassem em vigor e começassem a prejudicar com mais força os lucros do Irã com a venda de petróleo (SANGER, 2012) [20]

4.4 Conclusão

Diferente dos ataques cibernéticos supostamente realizados por *hackers* e simpatizantes russos contra a Geórgia em 2008, muitos deles com recursos amadores (vide capítulo 3), os ataques contra o Irã foram planejados e realizados por profissionais e equipes altamente qualificadas, especializadas neste tipo de operação. O resultado de tão grande investimento tanto financeiro quanto operacional surpreendeu o mundo quando descoberto: a partir daquele momento o Ciberespaço havia se tornado uma ameaça não só para os *softwares* (programas de computador) mas também para os *hardwares* (partes físicas) das instalações estratégicas. E a maneira como o stuxnet foi implantado nos equipamentos iranianos, que estavam totalmente desconectados do mundo externo, demonstra o que NYE JR defende na sua interpretação do exercício do poder no Ciberespaço (vide item 2.3): a interdependência complexa faz com que ninguém, nem mesmo uma instalação nuclear secreta, possa estar totalmente alheia aos recursos disponíveis na internet. Em algum momento o computador dos responsáveis

[20] tradução nossa, do original: " 'I don't think we have enough information,' Mr. Obama told the group that day, according to the officials. But in the meantime, he ordered that the cyberattacks continue. They were his best hope of disrupting the Iranian nuclear program unless economic sanctions began to bite harder and reduced Iran's oil revenues."

pela manutenção das instalações precisará acessar recursos externos para realizar o seu trabalho, e neste momento se abre uma janela para a infecção por um possível programa malicioso ("vírus"). Também, o aspecto militar e altamente profissional da sabotagem realizada (*hard power* definido por NYE JR, vide item 2.3) não desqualifica mas, pelo contrário, se completa com outros meios simultâneos e igualmente importantes para a obtenção do resultado desejado que era a interrupção do processamento de urânio pelo Irã. A diplomacia e a grande pressão internacional por parte de governos e da mídia (que poderiam ser classificados como *soft power* por NYE JR, vide item 2.3) demonstram que a visão realista não é mais única e preponderante no mundo altamente conectado de hoje, percepção esta que é totalmente coerente com a visão neoliberal para o poder no Ciberespaço (vide item 2.2c). É importante chamar a atenção também para o fato de que, embora os grandes atores envolvidos sejam Estados, o ataque se concretizou através da ação de atores menores mas que se tornam significativos dentro do Ciberespaço como *hackers*, grandes empresas, serviços secretos e outros. *Players* que adquirem considerável poder de ação individual devido à difusão de poder proporcionada pelo ambiente virtual (vide item 2.3) e que, neste caso, foram reunidos para constituir uma equipe que representa um nível muito alto de investimento, acessível talvez somente a Estados.

O ineditismo e novo precedente de ataque físico via ambiente virtual aberto pela arma cibernética criada, o vírus stuxnet, fazem do ataque às instalações nucleares de Natanz no Irã um marco no uso do Ciberespaço para o exercício de poder internacional, e sugerem o desenvolvimento de novas possibilidades de intervenção e coerção cibernética num futuro próximo, não só aos Estados mas também em empresas e instituições.

CONSIDERAÇÕES FINAIS

A importância crescente que o Ciberespaço assumiu para uma quantidade de atores bem distintos no cenário internacional durante a primeira década do XXI, viabilizando níveis diversos de ação e interatividade mundial até então inimagináveis em praticamente todas as áreas de atuação humana, fez com que os esforços para utilizá-lo como um instrumento de poder se tornassem uma tendência comum entre os seus usuários. E neste sentido, considerando-se a complexidade das relações internacionais que atualmente se desenvolvem através da grande rede mundial de comunicação digital que é a internet, a parte mais proeminente do Ciberespaço, constatamos que a perspectiva neoliberal de análise do poder cibernético é capaz de proporcionar uma compreensão mais abrangente e profunda das peculiaridades deste fenômeno do que, por exemplo, as visões idealista ou neorealista, isto por levar em conta muitas peculiaridades importantes que são ignoradas pelas outras linhas de análise abordadas, conforme explicado no capítulo 2. A visão neoliberal de NYE JR, explicitada no item 2.3, entende que a redução das assimetrias proporcionada pelo ambiente virtual para atores bem distintos em termos de poder econômico e político, tal como ativistas políticos e grandes partidos, pequenos grupos de interesse e governos, associações terroristas e organizações militares e até mesmo indivíduos e grandes empresas, sem falar nas poderosas instituições políticas organizadas através dos partidos majoritários, resulta numa difusão de poder inédita na história da humanidade. E este tipo de interpretação encontra forte ressonância em grande parte dos fatos observados durante a história recente, conforme demonstrado nos capítulos 3 e 4.

Não se pode ignorar a enorme importância que o Ciberespaço adquiriu para a estrutura política mundial na primeira década do século XXI e a boa compreensão deste momento ímpar, no qual houve uma rápida assimilação do ambiente virtual de comunicação pelas antigas e novas estruturas de poder internacionais, será vital para o entendimento das décadas seguintes porque muito do que acontece hoje no Ciberespaço pode ser interpretado como uma exacerbação das estratégias de poder cibernético que começaram a surgir nos primeiros anos deste século.

Também, a aceleração das interações entre as sociedades mundiais proporcionada pelo ambiente virtual representa uma nova perspectiva que ainda

está longe de ser bem compreendida academicamente. Conforme explicado no capítulo 1, muitas das transformações sociais impulsionadas pela troca fácil e rápida de informação a nível mundial continuam a acontecer de maneira dinâmica e cada vez mais acelerada, o que gera uma grande divergência de posições, pontos de vista e propostas teóricas entre os autores que pesquisam o assunto, causando, desta forma, significativas divergências entre as definições e termos específicos utilizados para descrever o fenômeno, terminando por levar a mais divergências e dificultando sobremaneira a construção de análises mais aprofundadas. Está claro que muito trabalho ainda precisa ser realizado para que tenhamos uma compreensão melhor sobre o que efetivamente representa o Ciberespaço para a política internacional.

Por fim, é importante ressaltar que as grandes transformações que o Ciberespaço trouxe para o exercício do poder no contexto internacional ainda convivem com as estruturas antigas tais como o poder militar e as grandes instituições políticas, e as maneiras com que elas fazem uso do ambiente virtual, conforme explicitado nos capítulos 3 e 4, estão em constante mutação, tanto no sentido de assegurar a sua continuidade quanto nas tentativas de silenciar ou controlar as novas estruturas de poder que vêm surgindo através da redução de assimetria proporcionada por este mesmo ambiente virtual, gerando assim ainda mais conflitos.

O estudo do exercício de poder no Ciberespaço aponta para um ambiente cada vez mais complexo composto por inúmeros interesses muitas vezes antagônicos mas nunca mutuamente exclusivos, e que se manifestam através de atores cada vez mais diversificados e ativos, dinamicamente influenciando o contexto internacional através do ambiente virtual. Dentro desta perspectiva, a preponderância do Ciberespaço como um catalizador de rápidas transformação sociais e, ao mesmo tempo, como mediador e deflagrador de conflitos em todo o planeta faz com que o seu estudo seja indispensável para uma compreensão mais ampla das forças políticas modernas.

REFERÊNCIAS BIBLIOGRÁFICAS

REFERÊNCIAS BIBLIOGRÁFICAS

Livros

ALBERTS, David S.; PAPP, Daniel S. **The Information Age**: An anthology on its Impacts and Consequences. CCRP Publication Series, 1997.

ARQUILLA, John.; RONFELDT, David. (Ed.). **Athena's Camp**: preparing for conflict in the information age. Santa Monica, CA: RAND Corporation, 1997. cap. 2.

CAVELTY, Myriam Dunn. The militarization of cyber security as a source of global tension. In: MOCKLI, Daniel (Ed.). **Strategic Trends 2012**. Zurich: Center for Security Studies (CSS), 2012.

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

CERUZZI, Paul E. **A History of Modern Computing**. 2. ed. London: The MIT Press, 2003.

GREATHOUSE, Craig B. Cyber War and Strategic Thought: Do the classic theorists still matter ? In: KREMER, Jan-Frederik; MÜLLER, Benedikt (Ed.). **Cyberspace and International Relations**: Theory, Prospects and Challenges. Heidelberg: Springer, 2014.

JACKSON, Robert; SORENSEN, Georg. **Introduction to International Relations Theories and Approaches.** 5. ed. Oxford: Oxford University Press, 2013.

KRAMER, Franklin D. Cyberpower and National Security: Policy Recommendations for a Strategic Framework. In: Kramer et al. **Cyberpower and National security.** Washington: National Defense University Press, 2009

KUEHL, Daniel T. From Cyberspace to Cyberpower: Defining the Problem. In: Kramer et al. **Cyberpower and National security**. Washington: National Defense University Press, 2009

KURBALIJA, J.; GELBSTEIN, E. **Gobernanza de Internet**: Asuntos, Actores y Brechas. Genebra, Suíça: Diplo Foundation, 2005.

NYE JR, Joseph S. Cyber Power. In. ____. **The Future of Power in the 21st Century**. Cambridge: Public Affairs Press, 2011.

SCHAAP, Arie J. **Cyber warfare operations**: Development and use under international law. Air Force Law Review, 2009.

SCHMITT, Michael N. (Ed.). **Tallinn Manual on the International Law applicable to Cyber Warfare**. New York: Cambridge University Press, 2013.

SINGER, P. W.; FRIEDMAN, Allan. **Cybersecurity and Cyberwar**: What everyone needs to know. New York: Oxford University Press, 2014.

STALLINGS, William. **Computer Security**: principles and practice. Boston: Pearson, 2012.

WALTZ, Kenneth. **Man, the State and War**. New York: Columbia University Press, 1959.

WEBER, Cynthia. **International Relations Theory**: A Critical Introduction. 3. ed. London: Routledge, 2010.

Artigos e Trabalhos Acadêmicos

ADETOKUNBO, Charles. **The future of internet security**. Association for Computing Machinery, New York, 31 out. 2002. Disponível em: < http://ubiquity.acm.org/article.cfm?id=763941 > Acesso em: 22 fev. 2017.

BEZERRA, Marcelo. **Artigo sobre Guerra Cibernética** "Cyberwar". DSIC/DSI-PR, Brasília, [2009]. Disponível em: < http://dsic.planalto.gov.br/artigos/71-artigo-sobre-guerra-cibernetica-qcyberwarq >. Acesso em: 9 jun. 2016.

BERNERS-LEE, Tim. **The World Wide Web**: Past, Present and Future. ago. 1996. Disponível em: < https://www.w3.org/People/Berners-Lee/1996/ppf.html > Acesso em: 21 fev. 2017.

BLUM, Douglas W. **The Russian-Georgian Crisis and Baku-Tbilisi-Ceyhan.** Program on New Approaches to Research and Security in Eurasia (PONARS), out. 2002. Disponível em: <http://www.ponarseurasia.org/sites/default/files/policy-memos-pdf/pm_0252.pdf> Acesso em: 17 abr. 2017.

BORCUCH et al. The Influence of the Internet on globalization process. **Journal of Economics and Business Research**, n. 1, 2012, p. 118-129. Disponível em: < http://www.uav.ro/jour/ index.php/jebr/article/download/348/pdf_111 > Acesso em: 21 fev. 2017.

MILANI, Carlos R S. Evolução Histórica da Cooperação Norte-Sul. In: Mello e Souza, André de. **Repensando a Cooperação Internacional para o Desenvolvimento**. Brasília: IPEA, 2014.

FOX et al. **One year later**: September 11 and the Internet. PewReasearchCenter, Washington, 5 set. 2002. Disponível em: < http://www.pewinternet.org/2002/09/05/one-year-later-september-11-and-the-internet/ > Acesso em: 22 fev. 2017.

HOLLIS, David. Cyberwar Case Study: Georgia 2008. **Small Wars Journal**, 6 jan. 2011. Disponível em: < http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008 > Acesso em: 17 abr. 2017.

IEG (Independent Evaluation Group). **The World Bank in Georgia 1993-2007**: Country Assistance Evaluation. World Bank, 2009. Disponível em <http://siteresources.worldbank.org/EXTCOUASSEVAL/ Resources/GeorgiaCAE.pdf>
Acesso em 17 abr. 2017.

KEOHANE, Robert O; NYE JR, Joseph S. What's New ? What's Not ? (And So What ?). **Foreign Policy**, n. 118, primavera 2000, p. 104-119

MUELLER, Paul; YADEGARI, Babak. **The Stuxnet Worm**. Disponível em: < http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf >. Acesso em: 10 jun. 2012.

KERR, Paul K. **Iran's Nuclear Program**: Status. Congressional Research Service. 17 out. 2012. Disponível em: < https://fas.org/sgp/crs/nuke/RL34544.pdf >. Acesso em: 09 jun. 2012.

RIOS, Maria J. et al. **The Georgia's Cyberwar.** Disponível em: < http://repositorio.ucp.pt/bitstream /10400.14/16726/1/the%20georgia%20cyberwar.pdf > Acesso em: 20 mai. 2017.

SQUASSONI, Sharon. **Iran's Nuclear Program**: Recent Developments. CRS Report for Congress, 6. set. 2006. Disponível em: < https://fas.org/sgp/crs/nuke/RS21592.pdf >. Acesso em: 09 jun. 2012.

SWARTZ, Aaron. **Guerilla Open Access Manifesto**. jul. 2008. Disponível em: < https://archive.org/ stream/GuerillaOpenAccessManifesto/Goamjuly2008_djvu.txt >. Acesso em: 20 fev. 2016.

TOPCHISHVILI, Roland. Ethnic Processes in Shida Karthli (The Ossetians in Georgia). In: **Causes of War, Prospects for Peace.** Tibilisi: Konrad-Adenauer-Stiftung, 2009. Disponível em: <http://www.kas.de/wf/doc/kas_18802-544-2-30.pdf>. Acesso em: 17 abr. 2017.

Periódicos

Associated Press. IAEA: Syria tried to build nuclear reactor. **Y Net News**, Tel Aviv, abr. 2011. Disponível em < http://www.ynetnews.com/articles/0,7340,L-4062001,00.html > Acesso em: 25 set. 2016.

ANDERSEN, Kurt. The best decade ever ? The 1990s, obviously. **The New York Times**, New York, 6. fev. 2015. Disponível em: < https://www.nytimes.com/2015/02/08/opinion/sunday/the-best-decade-ever-the-1990s-obviously.html?_r=0 > Acesso em: 16 fev. 2017.

BAYATLI, Tamam. Tankers Finally Leave Ceyhan Port for World Markets. **Azerbaijan International**, outono 2006, p. 92-95. Disponível em < http://www.azer.com/aiweb/categories/magazine/ai143_folder/143_articles/143_bp_developments.html > Acesso em 17 abr. 2017.

BIRNBAUM, Michael. Spurned by the West, Georgians look to Russia despite past quarrels. **The Washington Post**, Washington, 04 jul. 2015. Disponível em < https://www.washingtonpost.com/world/europe/despite-past-quarrels-with-russia-georgians-are-returning-to-its-orbit/2015/07/01/40d64c24-1b49-11e5-bed8-1093ee58dad0_story.html?utm_term=.53f3dec4eff0 > Acesso em: 24 mai. 2017.

CAVELTY, Myriam Dunn. Cyberwar: concept, status quo, and limitations. **Center for Security Studies (CSS),** ETH Zurich, n. 71, abr. 2010. Disponível em: < http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analyses-71.pdf > Acesso em: 19 mai. 2016.

ERDBRINK, thomas. Iran Confirms Attack by Virus That Collects Information. **The New York Times**, New York, 29. mai. 2012. Disponível em: < http://www.nytimes.com/2012/05/30/world/middleeast/iran-confirms-cyber-attack-by-new-virus-called-flame.html > Acesso em: 09 jun. 2016.

FARRELL, H. The Political Science of Cybersecurity III - How International Relations Theory Shapes U.S. Cybersecurity Doctrine. **The Washington Post**, Washington DC, 23 jan. 2014. Disponível em: < https://www.washingtonpost.com/news/monkey-cage/wp/2014/02/20/the-political-science-of-cyber security-iii-how-international-relations-theory-shapes-u-s-cybersecurity-doctrine/ > Acesso em: 29 out. 2015.

FRIEDMAN, George. The Russo-Georgian War and the Balance of Power. **Stratfor Worldview**, Austin, Texas, USA, 12 ago. 2008. Disponível em < https://www.stratfor.com/weekly/russo_georgian_war_and_balance_power > Acesso em 24 mai. 2017.

FLEMING, Ryan. Bits before bombs: How Stuxnet crippled Iran's nuclear dreams. **Digital Trends**, 2 dez. 2010. Disponível em: < http://www.digitaltrends.com/computing/bits-before-bombs-how-stuxnet-crippled-irans-nuclear-dreams/#ixzz4Wj6IzmS5 > Acesso em: 29 out. 2015.

HARMON, Amy. Recording Industry Goes After Students Over Music Sharing. **The New York Times**, New York, 23 abr. 2003. Disponível em: < http://www.nytimes.com/2003/04/23/us/recording-industry-goes-after-students-over-music-sharing.html > Acesso em: 06 jun. 2016.

HERSH, Seymor M. **A Strike in the Dark**. The New Yorker, Fev. 2008. Disponível em < http://www.newyorker.com/magazine/2008/02/11/a-strike-in-the-dark > Acesso em: 25 set. 2016.

KNIGHT, Will. Why Aaron Swartz's Ideas Matter. **MIT Technology Review**, Cambridge, 14 jan. 2013. Disponível em: < https://www.technologyreview.com/s/509841/why-aaron-swartzs-ideas-matter/ > Acesso em: 20 jan. 2017.

MANJOO, Farhad. Fall of the Banner Ad: The Monster That Swallowed the Web. **The New York Times**, New York, 5 nov. 2014. Disponível em: < https://www.nytimes.com/2014/11/06/technology/personaltech/banner-ads-the-monsters-that-swallowed-the-web.html > Acesso em: 20 jan. 2017.

MARKOFF, John. Before the gunfire, Cyberattacks. **The New York Times**, New York, 12 ago. 2008. Disponível em: < http://www.nytimes.com/2008/08/13/technology/13cyber.html > Acesso em: 20 jan. 2017.

MOUAWAD, Jad. Conflict Narrows Oil Options for West. **The New York Times**, New York, 13. ago. 2008. Disponível em: < http://www.nytimes.com/2008/08/14/world/europe/14oil.html >. Acesso em: 09 jun. 2016.

PETERS, Justin. The Idealist: Aaron Swartz and the Rise of Free Culture on the Internet. **The New York Times**, New York, 8 jan. 2016. Disponível em: < https://www.nytimes.com/2016/01/10/books/review/the-idealist-aaron-swartz-and-the-rise-of-free-culture-on-the-internet-by-justin-peters.html > Acesso em: 20 jan. 2017.

PFANNER, Eric. British Put Teeth in Anti-Piracy Proposal. **The New York Times**, New York, 14 mar. 2010. Disponível em: < http://www.nytimes.com/2010/03/15/technology/15iht-piracy15.html > Acesso em: 20 jan. 2017.

SANGER, David E. U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site. **The New York Times**, New York, 10. jan. 2009. Disponível em: < http://www.nytimes.com/2009/01/11/washington/11iran.html >. Acesso em: 09 jun. 2016.

SANGER, David E. Obama order sped up wave of cyberattacks against Iran. **The New York Times**, New York, 1. jun. 2012. Disponível em: < http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0 >. Acesso em: 09 jun. 2016.

SANGER, David E. Iran Complies With Nuclear Deal; Sanctions Are Lifted. **The New York Times**, New York, 16. jan. 2016. Disponível em: < http://www.nytimes.com/2016/01/17/world/middleeast/iran-sanctions-lifted-nuclear-deal.html?action=click&contentCollection=International%20Business&module=RelatedCoverage&region=EndOfArticle&pgtype=article >. Acesso em: 12 jun. 2016.

SANGER, David E.; MAZZETTI, Mark. Israel Struck Syrian Nuclear Project, Analysts Say. **The New York Times**, New York, 14 out. 2007. Disponível em < http://www.nytimes.com/2007/10/14/washington/14weapons.html?_r=0 > Acesso em 28 nov. 2016.

SCHMIDT, Eric E.; COHEN, Jared. The Future of Internet Freedom. **The New York Times**, New York, 11 mar. 2014. Disponível em: < https://www.nytimes.com/2014/03/12/opinion/the-future-of-internet-freedom.html > Acesso em: 20 jan. 2017.

SHEKARAUBI, Shahrooz. Iran's Case against Stuxnet. **Foreign Affairs Magazine**, 18. mar. 2014. Disponível em: < http://theiranproject.com/blog/2014/03/19/irans-case-against-stuxnet/ > Acesso em: 09 out. 2015.

SHIELS, Maggie. Cyber war threat exaggerated claims security expert. **BBC News**, 16. fev. 2011. Disponível em: < http://www.bbc.com/news/technology-12473809 > Acesso em: 26 fev. 2017.

SINHA, shreeya; BEACHY, susan campbell. Timeline on Iran's Nuclear Program. **The New York Times**, New York, 2. abr. 2015. Disponível em: < http://www.nytimes.com/interactive/2014/11/20/world/middleeast/Iran-nuclear-timeline.html#/#time243_10809 >. Acesso em: 09/06/2016.

STRATE, Lance. The Varieties of Cyberspace: problems in definition and delimitation. **Western Journal of Communication**, v. 63, n. 3, 1999. Disponível em: < http://www.tandfonline.com/doi/abs/10.1080/10570319909374648 > Acesso em: 06 jun. 2016.

ZETTER, Kim. An unprecendented look at the stuxnet, the world's fist digital weapon. **Wired**, 3. nov. 2014. Disponível em < https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ >. Acesso em: 09/06/2016.

Páginas internet

BBC News. **South Ossetia profile.** 21 abr. 2016. Disponível em < http://www.bbc.com/news/world-europe-18269210 >. Acesso em 17 abr. 2017.

BRADLEY, Tony. **Zero Day Exploits**: Holy Grail Of The Malicious Hacker. Disponível em: < http://netsecurity.about.com/od/newsandeditorial1/a/aazeroday.htm >. Acesso em: 09 jun. 2016.

DARC (Danish Association for Research on the Caucasus). **The Georgian - South Ossetian Conflict.** 30 abr. 2009. Disponível em: < https://web.archive.org/web/20090430213436/http://www.caucasus.dk/chapter4.htm >. Acesso em 17 abr. 2017.

Government of Georgia. **Recent History**. 2014. Disponível em <http://gov.ge/index.php?lang_id=ENG&sec_id=193> Acesso em 8 abr. 2017.

HILBERT, M. **Digital Technology and Social Change** [Curso Online Gratuito da Universidade da Califórnia]. Disponível em < http://www.martinhilbert.net/digital-technology-social-change/ > Acesso em 04 jun. 2016.

IMF (International Monetary Fund). **World Economic Outlook Databases.** Disponível em: < http://www.imf.org/external/ns/cs.aspx?id=28 > Acesso em: 24 mai. 2017.

Internet Society. **Brief History of the Internet.** Disponível em: < http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet > Acesso em: 23 mai. 2016.

Internet World Stats. **Georgia.** Disponível em <http://www.internetworldstats.com/asia/ge.htm> Acesso em 14 abr. 2017.

NATO (North Atlantic Treaty Organization). **Relations with Georgia**. 30 mar. 2017. Disponível em: < http://www.nato.int/cps/en/natohq/topics_38988.htm > Acesso em 09 abr. 2017.

OEC (Observatory of Economic Complexity). **Russia.** Disponível em: < http://atlas.media.mit.edu/en/profile/country/rus/ > Acesso em: 24 mai. 2017.

SHANDKDHAR, Pavitra. **DOS Attacks and Free DOS Attacking Tools.** [S.l.], 26 dez. 2016. Disponível em: < http://resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/ > Acesso em: 17 jan. 2017.