UNIVERSIDADE FEDERAL DO PAMPA
CAMPUS SANTANA DO LIVRAMENTO
BACHARELADO EM RELAÇÕES INTERNACIONAIS

ARTHUR BOLFI FALCOSKI

O CIBERESPAÇO, A RÚSSIA E AS RELAÇÕES INTERNACIONAIS: O PODER CIBERNÉTICO DO KREMLIN E SUAS CONSEQUÊNCIAS GLOBAIS

Sant'Ana do Livramento
2017

ARTHUR BOLFI FALCOSKI

O CIBERESPAÇO, A RÚSSIA E AS RELAÇÕES INTERNACIONAIS: O PODER CIBERNÉTICO DO KREMLIN E SUAS CONSEQUÊNCIAS GLOBAIS

Trabalho de Conclusão de Curso apresentado como requisito para obtenção de grau de Bacharelado em Relações Internacionais pela Universidade Federal do Pampa – UNIPAMPA.

Orientador: Prof. Dr. Flávio Augusto Lira Nascimento

Sant'Ana do Livramento
2017

ARTHUR BOLFI FALCOSKI

O CIBERESPAÇO, A RÚSSIA E AS RELAÇÕES INTERNACIONAIS: O PODER CIBERNÉTICO DO KREMLIN E SUAS CONSEQUÊNCIAS GLOBAIS

Trabalho de Conclusão de Curso apresentado como requisito para obtenção de grau de Bacharelado em Relações Internacionais pela Universidade Federal do Pampa – UNIPAMPA.
.

Trabalho de Conclusão de Curso defendido e aprovado em: 08/12/2017.

Banca examinadora

_____

Prof. Dr. Flávio Augusto Lira Nascimento
Orientador
(UNIPAMPA)

_____

Prof.ª Dr.ª Kathiane Benedetti Corso
(UNIPAMPA)

_____

Prof.ª Dr.ª Kamilla Raquel Rizzi
(UNIPAMPA)

Ficha catalográfica elaborada automaticamente com os dados fornecidos
pelo(a) autor(a) através do Módulo de Biblioteca do
Sistema GURI (Gestão Unificada de Recursos Institucionais) .

327.172 Falcoski, Arthur Bolfi
F184c O CIBERESPAÇO, A RÚSSIA E AS RELAÇÕES INTERNACIONAIS: O PODER CIBERNÉTICO DO KREMLIN E SUAS CONSEQUÊNCIAS GLOBAIS / Arthur Bolfi Falcoski.
111 p.

Trabalho de Conclusão de Curso(Graduação)-- Universidade Federal do Pampa, RELAÇÕES INTERNACIONAIS, 2017.
"Orientação: Flávio Augusto Lira Nascimento".

1. Rússia. 2. Ciberespaço. 3. Relações internacionais. 4. Poder cibernético. 5. Cyberwarfare. I. Título.

AGRADECIMENTOS

Agradeço à Universidade Federal do Pampa, e em especial ao meu orientador Flávio Lira, que esteve junto comigo durante o processo de graduação. Também gostaria de agradecer ao professor e amigo Renatho Costa, um importante agente na formação acadêmica e intelectual. Cabe, também, agradecer aos professores Fábio Bento, Anna Carletti, Kamilla Rizzi, Rafael Schmidt e Rafael Balardin, sendo que todos estes foram, em algum momento, importantes vetores do desenvolvimento de pensamento crítico e do processo de evolução mental.

Agradeço, em especial, aos meus pais, Milton e Irani, que sempre estiveram ao meu lado e me apoiaram ao longo destes árduos anos de graduação. A participação destes foi essencial para realizar todas as atividades até o momento. Agradeço pela compreensão e pelo apoio constante, e espero poder retribuir eventualmente. Também agradeço carinhosamente à minha tia, Ângela, que é como uma segunda mãe, e minha avó, Adélia, que é um anjo. Assim como meus outros tios e tias, que sempre me apoiaram.

Agradeço, também, aos amigos que proporcionaram grandes memórias durante esses gloriosos anos de UNIPAMPA. Agradeço à Tiago Melo por sempre perder para mim, assim se tornando um importante fator de minha felicidade, assim como o não menos pior, Tulio Cezar Bunder. Além disso, agradeço os amigos Rodrigo Hidalgo, Holden Kwasnik, Guilherme Cremm, Rodrigo Nogueira e Caio Augusto, assim como Fernanda Trindade, Ibrahim Dib, Louise Tezza, Ingrid Guimarães e Diego Detoni. Também cabe citar Bruno Bernardo, que apesar das atividades obscuras, se mostrou como um importante amigo. Também agradeço aos amigos integrantes do grupo musical Crew Hidra Rap, Gabriel, Yan, Vinícius e Gustavo, que, no futuro, formarão a primeira banda brasileira *Kremlin-backed.*

Agradeço, também, ao meu amor, Jady Mondeque, que é minha companheira de sofrimentos e alegrias nos últimos anos. Somente através de nossa união é que foi possível passar por cima das diversas adversidades, para assim podermos aproveitar cada momento efetivamente e de maneira única. Agradeço por ter me aturado durante inúmeras crises, onde só você soube trilhar o caminho da minha mente para me ajudar a crescer, e em essência, me ensinou a ser uma pessoa melhor. Mesmo que não seja evidente por vezes, seus pensamentos e crenças afetaram positivamente meu desenvolvimento como pessoa de maneira inigualável, e por estas e outras coisas, lhe agradeço imensamente. Te amo. Cabe, por fim, agradecer ao meu lindo cãozinho, Jorgina, e sua irmãzinha, Caos. Em sua inocência, a vida parece ter mais sentido, exceto quando afetam o ambiente com odores exageradamente inexplicáveis.

“I think happiness is love”

Vladimir Putin

RESUMO

O presente trabalho busca apresentar uma melhor compreensão de como a ascensão do ciberespaço e da internet causou grandes mudanças nas sociedades contemporâneas, incluindo nas interações interestatais. Analisaremos como os Estados passaram a observar as questões de segurança cibernética, devido aos perigos que advém da conectividade de infraestruturas básicas ao ciberespaço. Ainda, observaremos como os variados atores internacionais, principalmente os Estados, passaram a agir para atingir determinados objetivos no ciberespaço, com efeitos reais nas relações internacionais como um todo, assim também podendo compreender melhor o que é o poder cibernético. Além disso, observaremos como a Rússia se tornou um dos principais proponentes nas relações cibernéticas internacionais, como isto aconteceu, assim como quais são as estratégias e a visão de Moscou das operações cibernéticas, bem como compreender os efeitos das ações promovidas pelo Kremlin e por outros agentes cibernéticos nas relações internacionais como um todo.

Palavras-chave: Ciberespaço; Poder cibernético, Internet, Infraestrutura, Rússia, Políticas cibernéticas; *Cyberwarfare*; Guerra informacional; Relações cibernéticas internacionais.

ABSTRACT

CYBERSPACE, RUSSIA AND INTERNATIONAL RELATIONS: THE KREMLIN'S CYBER POWER AND IT'S GLOBAL CONSEQUENCES

The present work seeks to present a better understanding of how the rise of cyberspace and the Internet caused great changes in contemporary societies, including inter - state interactions. We will look at how states have come to look at cybersecurity issues because of the dangers of basic infrastructure connectivity to cyberspace. Also, we will observe how the various international actors, especially the nation states, began to act to achieve certain goals in cyberspace, with real effects in international relations as a whole, thus also being able to better understand what cybernetic power is. In addition, we will look at how Russia has become a leading proponent in international cyber relations, how this happened, what Moscow's strategies and vision of cybernetic operations are as well as understanding the effects of actions by the Kremlin and other cybernetic agents in international relations as a whole.

Keywords: Cyberspace; Cyber power; Internet; Infrastructure; Russia; Cyber policies; Cyberwarfare; Informational war; International cybernetic relations.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

APT – *Advanced Persistent Threat*

BBC – *British Broadcasting Corporation*

CIA – *Central Intelligence Agency*

DDoS – *Distributed Denial of Service*

DNC – *Democratic National Committee*

DOD – *Department of Defense*

E-ISAC – *Electricity Information Sharing and Analysis Center*

EUA – Estados Unidos da América

FBI – *Federal Bureau of Investigation*

FGV – Fundação Getúlio Vargas

FSB - *Федеральная служба безопасности Российской Федерации*

IP – *Internet Protocol*

KGB - *Комите́т Госуда́рственной Безопа́сности*

NASA – *National Aeronautics and Space Administration*

NSA – *National Security Agency*

NTV – *Novoye Nezavisimoye Nashe*

ONG – Organização não governamental

OTAN – Organização do Tratado do Atlântico Norte

PLC – Programador Lógico Controlável

RT – *Russia Today*

SQL – *Structured Query Language*

URSS – União das Repúblicas Socialistas Soviéticas

VK - *Vkontakt*

VPN – *Virtual Private Network*

SUMÁRIO

1 Introdução

A ascensão do ciberespaço como uma importante zona de atuação de variados atores é de grande relevância pois constantemente altera as relações internacionais como as conhecemos. O presente trabalho tem como objetivo compreender a intensificação das atividades no ciberespaço, o que isto significa para as relações internacionais e como as grandes potências lidam com este novo cenário, observando o caso da Rússia, que têm atuado na internet e no ciberespaço para atingir certos objetivos estratégicos, assim impactando as relações internacionais. Ainda, observaremos como a Rússia passou a ser um dos principais atores cibernéticos e como passou a utilizar operações no ciberespaço como uma ferramenta de política externa e interna. Como objetivos específicos, entenderemos a incorporação do ciberespaço à várias infraestruturas essenciais na sociedade contemporânea, assim como os Estados lidam com a questão da ascensão da internet e do ciberespaço como um todo. Ainda, veremos as capacidades cibernéticas de variados atores hábeis, incluindo os Estados-Nações mais poderosos, para assim entendermos como é uma cyberguerra. Ainda, observaremos a evolução das capacidades de guerra informacional da Rússia ao revisitarmos as políticas internas de Vladimir Putin e Dimitri Medvedev, para então compreendermos como se deu a construção do poder cibernético russo, e por fim, compreender como os russos enxergam as operações cibernéticas, como e em que cenários as realizam e quais são os efeitos disto nas relações internacionais.

Analisaremos, neste trabalho, concepções do entendimento do ciberespaço para os Estados Nações, assim como uma visão generalizada obtida a partir de ferramentas online. Observaremos, através de fatos recentes e documentos governamentais como a evolução da simbiose entre o ciberespaço e a realidade está se intensificando e se tornando essencial para garantir e melhorar o funcionamento de estruturas e serviços básicos, como a distribuição de energia elétrica. Além disso, observaremos como o poder estatal passou a agir no ciberespaço, uma nova plataforma com ampla possibilidade de atuação, seja na questão do controle de informações que entram no país, seja na possibilidade de efetuar ataques cibernéticos contra outros atores e adquirir vantagens estratégicas. Observaremos, através de Nye e Maness, como o poder cibernético pode ser compreendido melhor, e quais são os principais atores nas relações cibernéticas internacionais. Ainda, observaremos através de documentos oficiais e de operações estatais como se deu a formação da sociedade contemporânea russa nas administrações de Vladimir Putin e Dimitri Medvedev, e observando documentos como, por exemplo, a doutrina

militar russa, realizando também uma contextualização com importantes conflitos internacionais, poderemos observar como o Kremlin passou a compreender a questão da informação no ciberespaço nas últimas décadas. Ainda, observamos, através de autores como Soldatov, como a FSB passou a desempenhar um importante papel na questão da inserção estatal russa no ciberespaço, e então, através da análise de eventos recentes, afirmações de oficias governamentais e estudos de companhias de cibersegurança como a SecureWorks e a Symantec, observaremos como Moscou passou a entender que as operações no ciberespaço seriam de extrema importância para realizar operações de política externa, assim como interna.

A metodologia utilizada neste trabalho será uma observação histórica de eventos recentes, e uma análise hipotética-dedutiva será realizada para desenvolver o trabalho e melhor realizar as considerações conclusivas. O levantamento de dados foi realizado através da utilização de notícias, de documentos oficiais governamentais e de afirmações de autoridades estatais e experts em determinadas áreas, assim como dados de estudos de companhias e empresas, assim tornando a análise documental como parte essencial para melhor compreendermos os eventos e situações aqui apresentados.

O trabalho se divide em três capítulos, além da introdução e das considerações finais. No primeiro capítulo observaremos como a ascensão do ciberespaço passou a ser extremamente importante nas sociedades contemporâneas, tanto pela capacidade de difusão da informação quanto pela conexão entre o ciberespaço e serviços de infraestrutura básica, como, por exemplo, distribuição de energia, questões eleitorais e cadastramento de cidadãos. Neste cenário, buscamos observar como os governos e governantes são afetados por ações no ciberespaço, assim como e de que maneira buscam promover suas próprias ações, ao observarmos os atos e efeitos do vazamento de dados da NSA proporcionado por Edward Snowden. Na sequência, observaremos como alguns serviços básicos de funcionamento de sociedades contemporâneas estão em processo de incorporação ao ciberespaço, notadas nos exemplos da ascensão das smart grids e das cidades inteligentes. Além disso, observaremos algumas vulnerabilidades destes sistemas e os possíveis efeitos negativos que esta incorporação ao ciberespaço podem ter como efeito. No segundo capítulo, observaremos como ações cibernéticas são operacionalizadas e quais são seus efeitos, ao observarmos ações protagonizadas por diversos atores com diversos interesses. Entenderemos as consequências das atividades de cyberwarfare, assim como entenderemos quais são as tais armas cibernéticas. Na sequência, observaremos, juntamente com teóricos da área, como podemos conceitualizar o poder cibernético para melhor entendermos as relações cibernéticas internacionais e os efeitos destas no mundo real, onde

vivemos. Para isto, observaremos o que são as capacidades cibernéticas, como evoluem, e os principais atores internacionais na área.

No terceiro capítulo, observaremos a atuação da Rússia neste cenário. Para compreendermos efetivamente, realizaremos uma contextualização da situação interna na Rússia desde a chegada de Vladimir Putin ao poder, em 1999. Ao compreendermos as características que moldaram a sociedade russa e como esta interagiu com a ascensão do ciberespaço nas últimas décadas. Além disso, observaremos a importância do sistema político atual em Moscou para que a Rússia de fato se tornasse uma potência cibernética, observando como Putin e Medvedev entendiam a questão do ciberespaço e como buscariam explorá-lo. Na sequência, observaremos os conceitos russos para o ciberespaço ao observarmos documentos oficiais e eventos que se deram durante a administração de Putin, também entendendo o papel da FSB na formulação das políticas do Kremlin para atuação no ciberespaço. Então, analisaremos como os russos passaram a compreender as operações cibernéticas como operações de grande efetividade a partir da guerra da Chechênia, e passaram, constantemente, a investir em operações cibernéticas e buscar atingir certos objetivos estratégicos através destas. Observaremos, por fim, os casos de operações cibernéticas que afetaram a Estônia, Geórgia, Ucrânia e Estados Unidos ao longo dos últimos dez anos, para por fim compreendermos como os russos passaram a utilizar suas armas cibernéticas para atingir objetivos de política interna e externa.

O desenvolvimento do ciberespaço em uma grande camada que envolveu as sociedades humanas logo se tornou um dos principais fatores na habilidade de melhorar a qualidade de vida e a infraestrutura em vários países. Neste cenário, é importante entendermos como os Estados passaram a enxergar o desenvolvimento desta plataforma, e logo poderemos notar uma rápida inserção de agentes estatais no ciberespaço para atingir variados objetivos. Ao observarmos as ações de Snowden, logo aprendemos que pelas suas características, a internet se tornou um campo onde a informação, incluindo informação criminosa, terrorista e opositora aos governos (mas não só ela, é claro), passaram a ser fácilmente divulgadas e promovidas, sendo assim um importante campo de debate político, principalmente ao observarmos o número de pessoas conectadas à rede. Em essência, o ciberespaço deu vida à era da informação em que hoje vivemos, e logo seria importante para governos e governantes que se adentrassem no ciberespaço para garantir, em certos casos de maneira exagerada, algum tipo de controle sobre o fluxo de informações. Parece, de fato, quase que natural o processo da "intervenção estatal",

mas o ciberespaço apresenta características muito únicas e os governos sofrem para que as coisas não fujam ao controle.

No entanto, ainda observamos que os Estados proporcionaram boa parte deste desenvolvimento, muito devido aos grandes benefícios de incorporar o ciberespaço à redes de infraestrutura essencial. A partir do momento em que os governos passaram a lidar com a infraestrutura conectada, parece ser natural imaginar que o processo de securitização da internet e do ciberespaço começaria. É essencial, portanto, observarmos que mesmo o ciberespaço tendo características anárquicas, e realmente, atores individuais possam exercer um grande poder, os Estados ainda detém a maioria dos recursos humanos e financeiros e o de facto poder legislativo, judicial e executivo, podendo eventualmente regulamentar, se apoiado por capacidades técnicas avançadas, o ciberespaço de maneira efetiva.

Neste cenário, grupos de hackers e hackers individuais ainda são bem poderosos, como é importante observarmos, mas os Estados ainda detém o maior poder cibernético por estes fatores citados acima, e a partir do momento que perceberam que poderiam também agir ofensivamente no ciberespaço, passaram a investir em poder cibernético. É importante observarmos as operações estatais no ciberespaço para compreendermos melhor como se dá a separação de ações individuais e de ações estatais, que visam atingir objetivos estratégicos nas relações internacionais. Neste contexto, observaremos a ascensão do poder cibernético estatal e em que situações estas armas e o cyberwarfare podem ser utilizados. Se pararmos para observar os eventos globais recentes, rapidamente perceberemos que boa parte do noticiário e de conteúdo acadêmico passou a discutir as interações interestatais no ciberespaço como sendo um importante fator das questões geopolíticas e geoestratégicas. É, portanto, importante que observemos o desenvolvimento da plataforma do ponto de vista da Rússia, uma das principais potências cibernéticas e que hoje, sob comando de Vladimir Putin, é importante proponente nas relações internacionais novamente.

Ao analisarmos o cenário interno da Rússia, seu sistema político e seu entendimento do que é e como lidar com o ciberespaço e a internet, poderemos melhor compreender os eventos recentes, como o vazamento de informações por Snowden, ou o vazamento de emails e o escândalo eleitoral nos Estados Unidos. Ainda, compreendendo as operações de Moscou, melhor poderemos nos preparar para o futuro das relações cibernéticas internacionais. Assim sendo, ao compreendermos o papel e a conexão do Kremlin com as operações cibernéticas globais, levando em conta as questões geopolíticas relacionadas, poderemos efetivamente entender como as grandes potências enxergam o ciberespaço e como este realmente se tornou

um importante mecanismo de aplicação de política externa. Em essência, portanto, compreender o entendimento e a atuação da Rússia no ciberespaço é essencial para compreendermos as relações internacionais contemporâneas, já que o ciberespaço passou a afetar o mundo real de maneira aparentemente irreversível. Ainda, é essencial que observemos o comportamento de Moscou e de outras potências no ciberespaço para que melhor compreendamos as vulnerabilidades de nossa atual sociedade que se conectou imensamente ao ciberespaço. Enquanto colhemos os frutos disto, também devemos nos preparar para melhor nos protegermos e evitarmos que sistemas básicos de convivência humana cotidiana não se tornem um perigo constante para nossa estabilidade social.

2 O ciberespaço e as nações

No decorrer deste trabalho, assim como em muitos outros textos acadêmicos ou notícias de jornais, por muitas vezes são utilizados termos como “ciberespaço”, “ciber-guerra”, “ciber-capacidades”, “ciber-guerrilha” e afins. Parece até que se tornou parte cotidiana da vida a utilização e normalização destes termos. Mas o que significa e o que é “ciberespaço”?

Agora foco de estudo e interesse de indivíduos, grupos, organizações, empresas e até mesmo estados-nações, o ciberespaço não tem definição concordada amplamente, também por ser um termo relacionado a algo recente na história humana, e podendo significar algumas coisas, necessita-se observar melhor alguns entendimentos sobre o ciberespaço. O Departamento de Defesa dos Estados Unidos (U.S Defense Department, DOD) classifica o ciberespaço assim:

> A global domain within the consistent informational environment in the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, embedded processors and controllers (DOD 2015).[1]

De maneira mais simplória, a Comissão Europeia, instituição que representa os interesses da União Europeia, classifica o ciberespaço sucintamente como “O espaço virtual no qual circulam os dados eletrônicos dos computadores ao redor do mundo”.[2] Já o Ministério de Defesa da Federação Russa classifica o ciberespaço como “sistemas de informação, redes de computadores como a internet e a mídia eletrônica de massa criaram um novo espaço global: o da informação”.[3]

Ainda, um usuário qualquer entre as 3,7 bilhões de pessoas com acesso à internet que digitar em seu buscador favorito “o que é ciberespaço”, provavelmente encontrará a definição no famoso site da Wikipedia, como muito se faz hoje:[4]

> Ciberespaço é um espaço existente no mundo de comunicação em que não é necessária a presença física do homem para constituir a comunicação como fonte de relacionamento, dando ênfase ao ato da imaginação, necessária para a criação de uma

[1] Nossa tradução: Um Domínio global dentro do ambiente informacional consistente na rede interdependente de infraestruturas de tecnologia da informação e dados residentes, incluindo a Internet, redes de telecomunicações, sistemas informáticos, processadores embutidos e controladores. Texto original disponível em: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[2] Mais informações em: http://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A52013JC0001

[3] Mais informações em: http://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle

[4] Internet Live Stats. Internet Users.
Disponível em: http://www.internetlivestats.com/internet-users/

> imagem anônima, que terá comunhão com os demais. É o espaço virtual para a comunicação que surge da interconexão das redes de dispositivos digitais interligados no planeta, incluindo seus documentos, programas e dados, por tanto não se refere apenas à infraestrutura material da comunicação digital, mas também ao universo de informações que ela abriga (WIKIPEDIA, 2017).[5]

Como é possível observar, não existe uma definição simples satisfatória, de três ou quatro palavras, para o que é o ciberespaço. Agências governamentais, institutos, organizações e indivíduos podem ter sua própria concepção de ciberespaço. Apesar de diferentes em detalhes, se analisarmos as variadas definições aqui utilizadas, logo perceberemos que existem pontos de comum acordo: O ciberespaço é um espaço virtual, composto pela rede de infraestruturas tecnológicas globais que criaram um espaço de armazenamento informacional através da internet e outras redes do tipo. É um espaço onde a comunicação floresceu, mas com características muito diferentes das plataformas que precederam o ciberespaço na comunicação, e além disto, parece criar um tipo de teia invisível ao redor de todos ao se tornar peça fundamental no funcionamento técnico de muitos aparelhos que passaram a ser utilizados diariamente por humanos e fundamentais para a composição de estruturas maiores.

Bryant (2009, p. 48) afirma que o conceito de espaço é composto por quatro pré-conceitos: Lugar, Distância, Tamanho e Rota. Segundo Bryant, o ciberespaço apresenta estas quatro características, e apesar de não conter materiais físicos dentro dele, esta é apenas uma questão de analogia. A relativização das coisas físicas pode ser feita se compararmos os métodos de estudo de décadas atrás aos de hoje: Os trabalhos acadêmicos, livros, artigos e provas não necessariamente precisam existir no espaço físico ao que os humanos se acostumaram para que sejam reais hoje. O ciberespaço é tão espaçoso quanto o espaço. O ciberespaço também apresenta lugar, distância, tamanho e rota, apesar de apresentar diferenças específicas e complexidades além do mero entendimento de lugar, por exemplo.

Então, isto significa que o ciberespaço é a mesma coisa que espaço? A resposta para esta pergunta pode ser sim, ou não. O ciberespaço, como dito anteriormente, tem as características de espaço, mas também apresenta conceitos e fatores muito diferentes ao que estamos acostumados. O ciberespaço, por definição, não encontrou uma convergência de ideais suficientemente bem elaboradas para que se concorde amplamente sobre o que é este espaço, mas se concorda em uma coisa: ele é composto pela rede interconectada de transmissores eletrônicos. Ao estudarmos um pouco mais sobre o ciberespaço, logo entenderemos que esta característica é uma das chaves para se compreender o funcionamento do mesmo: No

[5] Disponível em: https://pt.wikipedia.org/wiki/Ciberespa%C3%A7o

ciberespaço, tudo está conectado. Existem, é claro, inúmeras maneiras e técnicas para que se regulem as atribuições desta conexão no mundo real, mas em essência, o ciberespaço é de fato uma grande teia eletrônica que nos cercou, feita por nós mesmos.

O ciberespaço se mostra presente e envolvendo as sociedades, se tornando parte do dia a dia de boa parte dos indivíduos em um país. Na maioria dos países desenvolvidos, aparelhos eletrônicos se tornaram essenciais para a vida cotidiana. No caso da internet, a plataforma revolucionou o *modus operandi*[6] de muitos dos fatores funcionais de uma sociedade, como por exemplo reuniões e diálogos sociais, manuseamento de dados, formas de estudo e acesso à informação, entre outras funções básicas de uma comunidade. É comum hoje que na internet se tenha rápido acesso a qualquer tipo de informação ou pessoa que se faça disponível, e cada vez mais, devido a natureza da plataforma, o mundo vai se interconectando.

É neste cenário que surge um importante questionamento: A internet revoluciona o mundo, e o ciberespaço afeta a todas as pessoas envolvidas por ele. Este espaço, como anotado anteriormente, têm características distintas do espaço real, onde os humanos vivem, e problemas podem surgir a partir da interação destas duas plataformas. Por exemplo, um usuário acessando a internet tem a sensação de ter acesso a qualquer lugar e coisa do mundo, mas no mundo real, o dos Estados e governos, a convivência humana é baseada na divisão territorial entre os Estados-Nações. Em um espaço que, por vezes, aparenta ignorar a existência de certas regras de convivência em sociedades humanas, é importante analisar como o Estado deve agir para que a utilização deste espaço não comprometa questões internas de grande importância, e até mesmo como agir para garantir que a sua própria existência e funcionamento pleno continuem em atividade perante a uma possível reviravolta na simbiose ciberespaço-realidade.

Os Estados, ao proporcionarem e observarem o desenvolvimento deste ciberespaço, logo perceberam que o desenvolvimento da rede mundial de computadores poderia trazer alguns contratempos. Enquanto que essencial para a evolução humana, a revolução tecnológica pela qual passamos pode se tornar uma dor de cabeça para sistemas administrativos e ao sistema-mundo em que vivemos hoje. Exatamente pelas características fundamentais da internet, como o acesso à informação, a velocidade de ação-reação no espaço-tempo em comparação ao mundo real, a sensação de não existirem barreiras e as crescentes melhorias em equipamentos tecnológicos e em softwares que trazem cada vez mais facilidades tanto aos cidadãos comuns quanto aos seus governantes, a plataforma que é parte importante do ciberespaço pode apresentar graves problemas aos Estados.

[6] Modus operandi: modo de operar.

Um Estado tem autoridade política limitada ao território em que o consiste. Um Estado é inteiramente baseado em território. O Ciberespaço é invisível e cerca a todos, além disso, se tornou parte cotidiana da vida e do funcionamento de serviços. Como, então, um Estado deve agir neste novo cenário? A questão da cibersegurança, ou a segurança do Estado dentro do ciberespaço, se tornou pauta chave entre os Estados desenvolvidos e em desenvolvimento, já que atores internacionais não identificados ou identificados poderiam causar graves problemas internos a um Estado. Ausência de regulamentação, grandes diferenças nas leis de proteção ao indivíduo, características específicas da plataforma, como a propensão ao anonimato, facilidade em se contornar barreiras e a velocidade exacerbada das ações e ausência de burocracia formam um conjunto perigoso para um governo. Estas características da internet podem, por exemplo, causar algo que hoje é cotidiano: um usuário comum obtém e clona cartões de crédito roubados na internet e os utiliza para lavagem de dinheiro. As vítimas, cidadãos de um determinado Estado, podem ser vítimas de qualquer pessoa no mundo, e se os criminosos souberem o que fazem, dificilmente serão rastreados e encontrados. Na internet, o crime parece compensar. O Brasil, por exemplo[7], figura no segundo lugar na classificação mundial de países que sofrem fraudes bancárias online e *malware*[8] financeiro. 58% da população brasileira está conectada à internet, mas a legislação e regulamentação da plataforma é simplesmente ruim, para não dizer inexistente. A sociedade brasileira é vítima diariamente de crimes cibernéticos e o Estado parece inoperante frente a esses obstáculos.

Em questões como esta do caso brasileiro citado, o crime cibernético é cometido por indivíduos ou grupos de criminosos. Porém, para um Estado, estes problemas como fraude bancária e roubo de cartão de crédito podem parecer problemas mínimos se pensarmos em ações de grupos mais especializados ou até mesmo de outro Estado. Na Era da Informação, e principalmente nas democracias ocidentais, informações sigilosas valem ouro e o vazamento destas podem custar uma presidência ou a governabilidade. Estas informações hoje são todas interconectadas através de sistemas seguros do governo, mas não são imunes a grupos de *hackers* autônomos ou outros atores com capacidades técnicas. Por exemplo, nas eleições presidenciais dos Estados Unidos em 2016, o vazamento de informações sigilosas da campanha de Hillary Clinton afetou diretamente milhões de votos e podem ter sido causa direta da derrota da democrata no fim do ano.[9] O caso, além de ter parecido jogar fogo no debate político interno,

---

[7] El País. O problema do cibercrime no Brasil. Disponível em: https://brasil.elpais.com/brasil/2015/10/23/opinion/1445558339_082466.html

[8] Malware. Malware é caracterizado como software malicioso, que provoca danos aos computadores e sistemas.

[9] The Guardian. Top democrat e-mails hacked. Disponível em: https://www.theguardian.com/us-news/2016/dec/14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds

ainda causa ecos de caos e faz o presidente Donald Trump balançar no poder por acusações[10] de colusão com os russos para vencer as eleições. O caso apresentado é apenas um exemplo de como a era da informação é uma realidade tanto para cidadãos quanto para governantes, e no caso destes últimos, a conjuntura recente aponta para um cenário cada vez mais complexo. *Websites* como o Wikileaks divulgaram, nos últimos anos, uma série de escândalos desde esquemas de corrupção governamental em vários países até informação classificada e dados secretos de potências como os Estados Unidos. Grupos de *hackers* que colaboram com sites como o Wikileaks obtém variadas informações sobre governos e governantes de maneira ilegal, utilizando suas habilidades dentro da internet, protegidos pela invisível camada do ciberespaço. Neste novo mundo, os governantes ficam mais expostos, e a população de um país desenvolvido como os Estados Unidos pode interagir com este tipo de informação de maneira rápida e grandiosa. Como a internet é já uma plataforma quase que totalmente integrada com a vida cotidiana, principalmente das gerações mais novas, escândalos, vazamentos e informações negativas sobre determinados assuntos podem causar uma bola de neve no mundo da política. A atuação polêmica da Wikileaks, aos olhos do governo americano, é uma afronta ao Estado em si. Mike Pompeo, diretor da CIA, disse que "É hora de chamar a WikiLeaks do que ela realmente é: um serviço de inteligência não estatal hostil, muitas vezes instigado por atores estatais como a Rússia".[11]

Se entendida por muitos como uma organização benfeitora que busca trazer a verdade à tona em um mundo de esquemas e artimanhas políticas internacionais, a Wikileaks se apresenta como uma ameaça verdadeira aos olhos de um Estado hegemônico como os Estados Unidos. Se esquecermos por um momento o tipo de política que os legisladores em Washington comumente propõe, podemos dizer que a informação é uma arma de guerra contra a Casa Branca, e atores como a Wikileaks, que provém do ciberespaço, são elementos de extrema relevância na segurança nacional de um Estado, e portanto pauta-chave nas discussões do mais alto nível em um governo. É compreensível, que neste cenário, o Estado se sinta acuado e se prepare para agir dentro desta nova e curiosa plataforma: o ciberespaço.

Em 23 de junho de 2013, o avião que carregava Edward Snowden pousou em Moscou.[12] Edward Snowden era um analista de sistemas e ex-funcionário da CIA (*Central Intelligence*

---

[10] Washington Post. The Trump campaign's attempted collusion. Disponível em: https://www.washingtonpost.com/opinions/the-trump-campaigns-attempted-collusion/2017/07/10/7841c090-65b0-11e7-8eb5-cbccc2e7bfbf_story.html?utm_term=.2c084ac56c24

[11] PressTV. Disponível em: http://www.presstv.com/Detail/2017/07/21/529155/WikiLeaks-will-take-down-America-CIA-director

[12] The Guardian. Edward Snowden's plane lands in Moscow. 2013. Disponível em: https://www.theguardian.com/world/2013/jun/23/edward-snowden-arrives-moscow

Agency, agência do serviço secreto americano). Após trabalhar para a NSA (*National Security Agency*, agência de segurança nacional americana) por um período de tempo, em 20 de maio de 2013, Snowden embarcou em um avião rumo a Hong Kong e em junho do mesmo ano revelou milhares de documentos classificados da NSA para um grupo de jornalistas.[13] Jornais conceituados e de alcance global como o The Guardian e o The Washington Post publicaram vazamentos que incluíam a publicitação de um sistema de vigilância secreto por parte do governo americano em cidadãos de boa parte do mundo, incluindo os seus próprios.[14] [15] As revelações de Snowden mostraram que o governo americano, através da NSA e da CIA, estava monitorando ilegalmente muitos de seus cidadãos de todas as maneiras possíveis. Além disto, também revelou uma série de situações em que agências de inteligência norte-americanas espionaram líderes estrangeiros e figuras políticas de alto escalão, incluindo Angela Merkel, chanceler alemã e figura de liderança na União Europeia, grandes parceiros americanos no cenário internacional. Em agosto de 2017, Edward Snowden vive em Moscou, e lá encontrou refúgio da perseguição que os Estados Unidos proporcionaram após a revelação de seu vazamento das informações confidenciais. Os Estados Unidos foram expostos a uma grandiosa imagem negativa por parte de boa parte do mundo, e para evitar danos ainda maiores, o governo americano procurava capturar Snowden, e a Rússia surgiu como o único destino possível.

As revelações de Edward Snowden, apesar de serem de extrema importância para o contexto das relações internacionais, devem ser deixadas de lado por um breve momento. Ao analisarmos os fatos revelados e refletirmos sobre a inserção americana no ciberespaço, percebemos que apesar de a internet ser uma plataforma diferente do que estamos acostumados e os governos podem sofrer ao interagir com esta, os Estados-nações também utilizam de sua capacidade para agir dentro do ciberespaço. O programa de monitoramento global da NSA e de seus parceiros canadenses, britânicos e australianos é uma demonstração de como o Estado está agindo dentro do ciberespaço. Uma rede tão popular como a internet, com as características que tem, como a velocidade de ação-reação e o fácil acesso por estar interconectada parece ser o molde perfeito para um programa de espionagem. O governo americano utiliza tecnologias que se tornaram cotidianas para boa parte do mundo em prol de sua segurança e interesse ao por exemplo, forçar companhias telefônicas de lhes fornecer dados de ligações privadas entre dois

---

[13] The Guardian. Snowden leaves Hong Kong. 2013. Disponível em: https://www.theguardian.com/world/2013/jun/23/edward-snowden-leaves-hong-kong-moscow

[14] The Guardian. The NSA Files. 2013. Disponível em: https://www.theguardian.com/us-news/the-nsa-files

[15] The Washington Post. Snowden comes forward. 2013. Disponível em: https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html?utm_term=.700bec1eb827

ou mais aparelhos. Além disso, ainda espiona em uma quantidade gigantesca de cidadãos estrangeiros e líderes globais, incluindo parceiros econômicos, políticos e militares. Na internet, passou a monitorar e-mails e boa parte da vida online de milhões de indivíduos conectados à rede. O ciberespaço é que permite este tipo de ação forte, porém de aparência sutil, por parte do Estado. O investimento nestas tecnologias, como criação de *software* e *hardware* para aperfeiçoar este tipo de operação de vigilância, se mostra agora como uma boa estratégia, e em situações específicas, até mesmo uma abordagem mais assertiva pode ser originada a partir do momento em que um governo obtém este tipo de tecnologia. Na guerra da Geórgia, em 2008, o governo da Geórgia afirmou estar sob ataque cibernético com aparência de recursos ao nível de um Estado-nação.[16] Alguns serviços como a comunicação interna do governo pararam de funcionar. A inserção do Estado no ciberespaço é tanto para se defender, quanto para atacar. Ao ampliar sua presença no ciberespaço, o Estado está garantindo a sua própria segurança contra os inúmeros agentes hostis possíveis e também ampliando suas capacidades para adquirir algum tipo de vantagem estratégica, seja adquirindo informações ou seja danificando algum tipo de sistema conectado à rede.

Observamos como o Estado, agente pesado pelo tempo histórico, lento pelas suas demasiadas atividades burocráticas e possível candidato a desaparecimento viu a oportunidade e necessidade de se mobilizar dentro do ciberespaço. O ciberespaço é o que o Estado não é. Não tem território, não é burocrático. O ciberespaço preza pelo indivíduo e pelo anonimato, e ações dentro do mesmo ocorrem em uma diferente, muito superior, escala de espaço-tempo. Conforme o Estado, que ironicamente é o desenvolvedor desta plataforma, vai sendo envolvido pelo mundo virtual, novos desafios vão surgindo. Enquanto que ainda detenha poder legislativo vigente sobre os serviços de telecomunicação, a habilidade estatal de gerenciar elétrons, em comparação a outros setores, parece ser cada dia mais inoperante.

Ainda assim, o Estado se apresenta como o principal ator no sistema-mundo, e o desenvolvimento da internet e do ciberespaço está muito relacionado a ele. O Estado, para se desenvolver e sobreviver, agora explora de maneira grandiosa as capacidades tecnológicas que a sociedade vêm desenvolvendo para que novas maneiras de funcionamento de serviços sejam atingidas. Por exemplo, serviços de distribuição elétrica, serviços eleitorais, cadastramento de cidadãos, sistemas bancários, sistema de tráfego, serviços de distribuição de água e até mesmo serviços de cunho militar estão, agora, em Estados desenvolvidos, sendo melhorados,

[16] CNET. Georgia accuses Russia of coordinated cyberattack. 2008. Disponível em: https://www.cnet.com/news/georgia-accuses-russia-of-coordinated-cyberattack/

ampliados e alterados com componentes cibernéticos, como por exemplo o acesso à internet, ou aparelhos de comunicação de longa distância e adaptadores conectados ao ciberespaço. Enquanto que até o momento, neste trabalho, tenha sido apresentada uma visão negativa para o Estado do advento da revolução tecnológica, com o vazamento de informações classificadas e uma série de outros contratempos, a verdade é que o ciberespaço, se ignoradas as perigosas características anárquicas, vêm trazendo grandes melhorias aos sistemas de funcionamento de um país, estado ou região. O aperfeiçoamento de serviços básicos ou extremamente úteis é uma vitória tanto para um governo quanto para a população afetada por esta mudança, portanto quanto mais tecnologicamente avançados estes sistemas em um país, mais veremos a implementação destas mudanças ocorrendo. A questão que buscamos demonstrar na próxima seção é exatamente uma demonstração de como alguns desses sistemas, apesar de aperfeiçoados e mais práticos, por estarem conectados ao ciberespaço, podem apresentar um risco gravíssimo a um governo.

2.1 Os Estados e a crescente dependência em tecnologias cibernéticas

Smart City.[17] O nome é atrativo, e algumas características também. Hoje Amsterdam, Barcelona, Madrid e Manchester são alguns exemplos do que se considera uma "*smart city*".[18] Além de uma ótima propaganda, o termo está relacionado ao desenvolvimento da integração da tecnologia da informação e comunicação com uma área urbana, daí o nome: cidade inteligente. Em uma cidade inteligente, algumas funções e serviços da cidade são gerenciados ou manuseados através de sistemas computadorizados interconectados. Serviços de segurança, hospitais, sistemas de transporte, escolas, hospitais, distribuição de água, entre outros serviços, são alguns exemplos de serviços que podem ser melhorados ao estarem conectados a uma rede computadorizada. Por exemplo, o recolhimento de dados e informações para qualquer tarefa pode ser muito mais rápido e prático, aumentando grandiosamente a eficiência dos serviços governamentais fornecidos.[19]

Enquanto que uma cidade inteligente é algo inovador e com grandes benefícios para muitos dos envolvidos, incluindo governantes e a população, a questão que se levanta aqui é clara: Estes serviços básicos de funcionamento estão, agora inegavelmente, passando por um

[17] Tradução livre: Cidade Inteligente.
[18] Amsterdam Smart City. Amsterdam's City Projects. 2016. Disponível em: https://amsterdamsmartcity.com/
[19] MIT. Six lessons from Amsterdam's Smart City Initiative. 2016. Disponível em: http://sloanreview.mit.edu/article/six-lessons-from-amsterdams-smart-city-initiative/

processo de transição do mundo analógico para o mundo digital. Até que ponto estes sistemas interconectados são seguros? A resposta é incerta, ainda. É inegável que as cidades inteligentes são um exemplo de interação entre as novas tecnologias humanas e um conceito básico da sociedade, a área urbana de convivência. Neste cenário, a tendência é de que exatamente pelos grandes benefícios que se apresentam, esta interação seja realizada com muito mais frequência e de maneiras ainda mais abrangentes.

Estas tecnologias estão conectadas ao ciberespaço. As cidades estão se tornando parte do mundo digital. E como observamos, as regras do mundo digital são ligeiramente diferentes das do mundo real, e problemas sérios podem surgir para uma plataforma nova como o conceito de cidade inteligente. Ainda que estes sistemas sejam seguros, conforme as tecnologias vão avançando, a possibilidade de uma falha sistêmica também vai. A partir do momento que uma *smart city* se conecta ao ciberespaço, ela pode abrir uma porta relativamente perigosa. Se houver alguma falha de segurança, ou até mesmo sem haver falha alguma, estes mesmos serviços básicos de funcionamento que estão sendo melhorados podem sofrer golpes catastróficos. Imagine, por um momento, um sistema de metrô totalmente computadorizado: as possíveis consequências de um ciber-ataque neste causam arrepios na mente. Claro, as cidades inteligentes e as tecnologias digitais têm algumas camadas de proteção, mas conforme o nível de interconectividade aumenta, os perigos também aumentam. As cidades inteligentes são um exemplo de como os serviços governamentais e de utilidade pública, assim como a sociedade como um todo, estão interagindo com a nova plataforma cibernética que se apresentou nas últimas décadas. Agora, veremos um caso onde esta interação causou danos bilionários a um Estado-nação.

Em 29 de novembro de 2011, o então presidente iraniano Mahmoud Amahdinejad afirmou que centrífugas de enriquecimento nuclear de grande importância para o programa nuclear iraniana foram comprometidas por um vírus de computador.[20] O que hoje é conhecido internacionalmente como o vírus Stuxnet invadiu os sistemas computadorizados de uma usina nuclear em Natanz, no Irã, e após uma série processos, acabou inviabilizando o funcionamento de boa parte do programa nuclear iraniano e destruindo uma quantidade considerável de centrífugas nucleares.

O *malware* nomeado de Stuxnet é, até os dias de hoje, uma grande incógnita. O vírus de computador extremamente bem desenvolvido atuava de maneira sutil, porém eficiente: o

[20] Der Spiegel. Iran's nuclear program hit by computer virus. Disponível em: http://www.spiegel.de/netzwelt/gadgets/irans-atomprogramm-ahmadinedschad-raeumt-virus-attacke-ein-a-731881.html

malware infectou uma quantidade muito grande de computadores do mundo todo.[21] Uma parte de variadas indústrias, como por exemplo de distribuição de energia[22] e de telecomunicações, inclusive norte-americanas[23], afirmou ter sido infectada pelo vírus ao longo de 2010 e promoviam temores de uma possível falha nos serviços, afirma Kim Zetter, especialista em cibersegurança.[24] Porém, analistas da Symantec, companhia de cibersegurança, afirmam, no documentário "Zero Days", que perceberam que o código malicioso procurava por algum tipo de alvo específico. Ao perceber-se que o Irã era o país mais infectado do mundo, logo se notou que o alvo poderia ser Teerã.

O Stuxnet buscava afetar explicitamente um *hardware* desenvolvido pela Siemens: um PLC, ou um controlador lógico programável em português.[25] Apesar de o vírus ter se espalhado grandiosamente, o objetivo específico do código era afetar diretamente os controladores da Siemens. O PLC é um aparelho que promove a automação de processos elétricos como a linha de produção em fábricas, e centrífugas que enriquecem material nuclear e é conduzido pelo software da Siemens instalado em computadores com o sistema operacional Windows. Em síntese, o vírus invade o PLC e modifica a frequência de transmissão para os motores de máquinas alterando a velocidade de rotação destes, causando, em última instância, a falha e/ou destruição do motor, isto permitido pela intrusão do Stuxnet nos computadores com Windows, inabilitando o software e a conexão com os PLCS.

As centrífugas iranianas começaram a falhar meses antes da descoberta da causa, e a conexão entre as falhas e os aparelhos da Siemens que as centrífugas utilizavam era desconhecida. Quando os iranianos descobriram que haviam sido vítimas de um ataque cibernético, logo acusaram os Estados Unidos e Israel de estarem envolvidos no esquema.[26] De fato, especialistas em cibersegurança da Simantec e do Kaspersky Lab afirmaram que somente um estado-nação poderia estar por trás deste tipo de código malicioso como o Stuxnet, que é extremamente complexo e sem erros. Eugene Kaspersky, fundador da Kaspersky, afirmou em entrevista ao documentário "Zero Days" que um grupo de *hackers* autônomo, ou hacktivistas

---

[21] FT. Stuxnet causes worldwide alarm. 2010. Disponível em: https://www.ft.com/content/cbf707d2-c737-11df-aeb1-00144feab49a?mhq5j=e6

[22] BusinessInsider. US and European Energy Companies hit by cyberweapon. 2014. Disponível em: http://www.businessinsider.com/energetic-bear-virus-and-energy-companies-2014-7

[23] WSJ. Virus infects Chevron Network. 2012. Disponível em: https://www.wsj.com/articles/SB10001424127887324894104578107223667421796

[24] ZETTER, Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's first digital weapon. Broadway Books, 2015.

[25] The Telegraph. How Stuxnet works. 2011. Disponível em: http://www.telegraph.co.uk/technology/8274488/How-Stuxnet-works-what-the-forensic-evidence-reveals.html

[26] The Guardian. Iran accuses Siemens of helping US and Israel with Stuxnet. 2011. Disponível em: https://www.theguardian.com/world/2011/apr/17/iran-siemens-stuxnet-cyber-attack

organizados, não teriam capacidade para gerar um código deste nível, que envolveria uma série de recursos caros para ser uma realidade, a ponto de que somente um Estado-nação poderia desenvolver tal arma.[27] Um destes recursos é o descobrimento e utilização de um chamado "*zero day exploit*", ou seja, quando os *hackers* descobrem uma falha de segurança em um sistema como o Windows logo após a atualização mais recente. Estas falhas podem valer milhões de dólares para a companhia e para os possíveis invasores.

O próprio fato do foco do *malware* ser especificamente um tipo de aparelho utilizado no programa nuclear iraniano, e levando-se em conta também o claro cunho de sabotagem do vírus, entende-se que os programadores do Stuxnet não buscavam o lucro. Isto somado à complexidade do *malware* e aos depoimentos de especialistas internacionais promove uma importante discussão sobre o envolvimento de um Estado-nação nesta questão. De fato, um código tão específico pode levar anos para ser produzido, e o fato de que o Stuxnet não apresenta *bugs* é algo fascinante no mundo da cibersegurança. Somente um grupo extremamente capacitado, focado e com muitos recursos poderia desenvolver um código tão sofisticado, ainda mais levando-se em conta o alvo e o contexto geopolítico global.

O Irã acusou mais de uma vez os Estados Unidos e Israel de serem responsáveis pela criação e aplicação do Stuxnet, e análises de especialistas, assim como o comportamento de oficiais dos países ser no mínimo suspeito, indicam algum tipo de conexão entre os Estados Unidos e Israel com o poderoso *malware*.[28] No documentário de Alex Gibney, "Zero Days", que conta a história do *malware* aos olhos de especialistas e oficiais do governo, são apresentados agentes secretos dos Estados Unidos trabalhando para a NSA, dando depoimentos sem revelar a identidade. Estes supostos agentes afirmam ter sido parte da equipe que desenvolveu o *malware* Stuxnet, que chamam de arma cibernética. Os agentes afirmam que o Stuxnet foi desenvolvido pelos governos dos EUA e de Israel para conter o programa nuclear iraniano, porém as agências perderam o controle do *malware* quando os israelenses se precipitaram e lançaram o vírus, que enquanto foi de fato efetivo, acabou infectando aliados e poderia ter sido mais forte ainda. Ainda, neste documentário, uma série de oficiais governamentais e do alto-escalão das agências de inteligência norte-americanas e do Mossad dão a entender algum tipo de participação na criação do vírus.

De fato, enquanto que as informações e as especificidades do caso ainda não são completamente claras, os ataques do Stuxnet ao programa nuclear iraniano vieram em um

[27] Fonte: Alex Gibney. Zero Days. 2016. 1h56min.

[28] NY Times. Israeli test on worm called crucial in Iran nuclear delay. Disponível em: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?mcubz=3

momento de grandes divergências internacionais para Teerã. O governo iraniano estava em um impasse com o governo americano, que se opunha fielmente à expansão do programa nuclear iraniano, e acusava os iranianos de estarem planejando desenvolver armas nucleares em segredo. Os israelenses eram ainda mais assertivos, sempre com discursos que davam a entender que os dois países estavam em pé-de-guerra, defendiam atitudes mais agressivas perante ao programa de enriquecimento de urânio iraniano. O governo americano, em parceria com os israelenses, tratava como prioridade a resolução da questão nuclear iraniana, e coincidentemente, importantes cientistas nucleares iranianos foram assassinados em mais de uma ocasião em Teerã nos últimos anos.[29] Se colocarmos estes fatos em contextualização com o lançamento do Stuxnet e como o ataque cibernético se deu, podemos observar que os americanos e israelenses estavam no mínimo satisfeitos pelos fatos ocorridos, e o envolvimento chega a ser óbvio.

O Irã foi vítima de um poderoso ciberataque, e os proponentes deste, muito possivelmente, foram outros Estado-nações. Para Teerã, o programa nuclear é uma prioridade, e os recursos investidos neste são altos e constantes.[30] Para o governo, a energia nuclear, seja para um fim ou outro, é essencial, e mesmo com todas as camadas de segurança, foi vítima de um ataque partindo do ciberespaço. Entende-se que o Stuxnet foi a primeira ciberarma desenvolvida, provavelmente, por um Estado-nação, sendo assim a precursora de um novo tipo de guerra: a guerra cibernética. Além de afetar diretamente uma infraestrutura essencial para o governo local, o *malware* ainda saiu de controle e demonstrou o quão perigoso o mundo cibernético pode ser ao interagir com o mundo real.

O caso iraniano é uma clara demonstração de como o chamado *cyberwarfare*[31] é uma realidade. Se uma centrífuga de enriquecimento de urânio está conectada ao ciberespaço, outros vários sistemas também podem estar. É o caso do sistema de distribuição de energia elétrica. No mundo todo, a dependência de energia elétrica da sociedade contemporânea se tornou uma realidade décadas atrás, e esforços em realizar, ampliar e aperfeiçoar o sistema de distribuição desta dentro de vários países foram aumentando conforme os anos passaram. Não demorou para que surgisse o conceito de "*smart grid*", ou grade inteligente em português, o que caracteriza, em resumo, um sistema de distribuição elétrica aperfeiçoado pelas inovações tecnológicas que ocorreram e ainda estão ocorrendo na era digital. Hoje, o conceito de *smart grid* é uma

[29] The Guardian. Iran nuclear scientist killed in bomb attack. Disponível em: https://www.theguardian.com/world/2010/nov/29/iran-nuclear-scientist-bomb-attack

[30] ICG. Key features of Iran's Nuclear Program. 2015. Disponível em: http://blog.crisisgroup.org/worldwide/2015/09/10/key-features-of-irans-nuclear-program/

[31] Cyberwarfare: A combinação das capacidades cibernéticas e a operacionalização destas em cenário de guerra

realidade: O Energy Independence and Security Act of 2007 (Ato de Independência e Segurança da Energia de 2007) fez com que a instalação de uma rede elétrica inteligente, moderna e digital fosse uma política pública federal nos Estados Unidos, e garantiu investimentos e criação de grupos específicos para o desenvolvimento desta.

Nos Estados Unidos, a implementação de uma "*Smart Grid*" se tornou prioridade no governo Obama. No texto que virou lei a definição de "*smart grid*" é esta:[32]

> It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterize a Smart Grid: (1) Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid. (2) Dynamic optimization of grid operations and resources, with full cyber-security. (3) Deployment and integration of distributed resources and generation, including renewable resources. (4) Development and incorporation of demand response, demand-side resources, and energy-efficiency resources. (5) Deployment of `smart' technologies (real-time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices) for metering, communications concerning grid operations and status, and distribution automation. (6) Integration of `smart' appliances and consumer devices. (7) Deployment and integration of advanced electricity storage and peak-shaving technologies, including plug-in electric and hybrid electric vehicles, and thermal storage air conditioning. (8) Provision to consumers of timely information and control options. (9) Development of standards for communication and interoperability of appliances and equipment connected to the electric grid, including the infrastructure serving the grid. (10) Identification and lowering of unreasonable or unnecessary barriers to adoption of smart grid technologies, practices, and services (US GOVERNMENT, 2007).[33]

Como se pode observar, as características por definição da "*smart grid*" apresentam uma composição específica de entes ligados ao ciberespaço: O uso de informação digital, a dinamização da operação de distribuição através da instalação de sistemas mais modernos,

---

[32] U.S Government. Public Law no. 110-140 (19/12/2007). Disponível em: https://www.congress.gov/bill/110th-congress/house-bill/6/text

[33] Nossa tradução: É a política dos Estados Unidos apoiar a modernização do sistema de distribuição e transmissão de eletricidade da Nação para manter uma infra-estrutura de eletricidade confiável e segura que possa atender ao crescimento da demanda futura e alcançar cada um dos seguintes, que juntos caracterizam uma Grade Inteligente: (1) Aumento do uso da tecnologia de informação e controle digital para melhorar a confiabilidade, segurança e eficiência da rede elétrica. (2) Otimização dinâmica de operações e recursos da rede, com ciber-segurança total. (3) Implantação e integração de recursos e geração distribuídos, incluindo recursos renováveis. (4) Desenvolvimento e incorporação de resposta à demanda, recursos do lado da demanda e recursos de eficiência energética. (5) Implantação de tecnologias "inteligentes" (tecnologias em tempo real, automatizadas e interativas que otimizam a operação física de aparelhos e dispositivos de consumo) para medição, comunicações relativas a operações e status da rede e automação de distribuição. (6) Integração de aparelhos "inteligentes" e dispositivos de consumo. (7) Implantação e integração de tecnologias avançadas de armazenamento de eletricidade e pico de barbear, incluindo veículos elétricos elétricos e híbridos plug-in e ar condicionado de armazenamento térmico. (8) Proporcionar aos consumidores informações oportunas e opções de controle. (9) Desenvolvimento de padrões de comunicação e interoperabilidade de aparelhos e equipamentos conectados à rede elétrica, incluindo a infra-estrutura que atende a grade. (10) Identificação e redução de barreiras não razoáveis ou desnecessárias à adoção de tecnologias, práticas e serviços de rede inteligentes.

conectados a aparelhos eletrônicos e de alto alcance para melhorar a tanto a oferta de energia quanto a demanda por esta. Uma rede elétrica inteligente é composta pela rede tradicional de distribuição de energia elétrica e aperfeiçoada pela instalação de *hardware* capacitor, como por exemplo, um medidor inteligente.[34] O medidor inteligente é um aparelho eletrônico que permite o registro de informações em intervalos de tempo muito curtos e comunica estas informações automaticamente à central para cobranças e monitoramento. Esta central em uma determinada rede elétrica inteligente também conta com uma série de aparelhos automatizados para que o processo se torne mais rápido, prático, além de mais confiável. Além destas melhorias, vários outros sistemas foram implementados em o que é entendido como uma "*smart grid*", e estes sistemas, em boa parte, estão conectados ao ciberespaço. Enquanto que as melhorias são visíveis e os benefícios claros, existem algumas certas preocupações com este novo sistema. Além de afetar diretamente as questões de privacidade, já que os dados coletados permitem que alguém com as informações corretas mapeie claramente algum tipo de ação organizada ou rotina de vida e poderia ser utilizado por terceiros para fins obscuros, o medidor inteligente apresenta uma perigosa ferramenta: Ele está conectado ao ciberespaço e apresenta um sistema instantâneo de desligamento da energia que está sendo fornecida em determinado local se o sistema assim entender que deve ser. Por exemplo, no caso de uma conta atrasada demasiadamente, o medidor é que executa o corte de energia. Este mecanismo instantâneo pode ser controlado à distância, já que está conectado ao ciberespaço, sendo um sistema eletrônico de dados. Os perigos de haver uma invasão ou algum tipo de comprometimento do pleno serviço são reais e causam grande preocupação nas autoridades. Em tese, uma ação coordenada poderia causar grandiosos danos à uma cidade, região ou até mesmo país.

Em 23 de dezembro de 2015, trabalhadores no centro de distribuição da Prykarpattyaoblenergo, uma companhia de distribuição de energia elétrica para o oeste da Ucrânia, observaram enquanto os cursores de seus computadores se moviam de maneira autônoma na tela. Ao tentarem interagir com o aparelho, não havia resposta na tela do computador. O que era curioso no início, logo se tornou caótico: O computador começou a desativar disjuntores em várias subestações e tornar inoperantes estas subestações de distribuição. Os operadores perderam completamente o controle do sistema em poucos minutos, e 230 mil pessoas já estavam sem energia. Os hackers responsáveis pela ação derrubaram os sistemas reservas de energia das subestações e do centro da companhia, deixando no escuro até

[34] US Government. What is a smart grid? 2016. Disponível em: https://www.smartgrid.gov/the_smart_grid/smart_grid.html

mesmo os trabalhadores da empresa, causando pânico generalizado entre estes.[35] A energia da área afetada, em geral, ficou desligada por apenas algumas horas, mas os danos em alguns aparelhos eletrônicos foram permanentes, e algumas das subestações demoraram a voltar a funcionar. Ainda, causou danos que apenas foram reparáveis através de operação manual dos aparelhos através de um sistema de *backup*. Nos Estados Unidos, por exemplo, estes sistemas manuais estão deixando de existir.[36] A E-ISAC (*Electricity Information Sharing and Analysis Center*), uma ONG de cibersegurança, confirmou as informações do governo da Ucrânia de que este ataque se tratou de um ciberataque de recursos grandiosos.[37] Não demorou para que Kiev apontasse os dedos para Moscou, já que boa parte das investigações locais apontou que usuários russos agiram no ataque.[38] [39] Moscou negou as acusações, assim como a Ucrânia negou envolvimento oficial na sabotagem de uma série de linhas de eletricidade que causaram falta de energia em toda a Crimeia, um mês antes dos ataques cibernéticos na Ucrânia.[40]

A energia elétrica em boa parte da Ucrânia ocidental foi cortada devido a uma intrusão ilegal nos sistemas eletrônicos de distribuição de energia. A "*grid*" ucraniana foi vítima do primeiro grandioso ciberataque em uma estrutura básica de funcionamento de uma sociedade, abrindo caminho para os maiores temores em relação a isto. Em sistemas como a "*smart grid*" norte-americana, o grau de integração do mundo digital com o próprio sistema é essencialmente superior ao da rede ucraniana, e apesar de ter equipamentos mais avançados, uma falha ou intrusão poderia ser mais catastrófica. Isto se deve ao fato de que por exemplo, na Ucrânia, durante os ciberataques, *backups* manuais foram operados para garantir um pouco de funcionalidade à rede, e eventualmente salvar parte dela. Nos Estados Unidos, estes *backups* vão cada dia sendo mais raridade em subestações de distribuição de energia. Um ataque de sucesso poderia causar uma pane geral.

Esta situação, portanto, nos diz mais: O funcionamento da rede de energia elétrica, um serviço básico e fundamental, em um país europeu, foi diretamente afetado por uma intrusão

---

[35] Forbes. Inside Ukraine's power outage. Disponível em: https://www.forbes.com/sites/thomasbrewster/2016/01/04/ukraine-power-out-cyber-attack/#27f158416fa8

[36] US Government. NIST. Guidelines for Smart Grid Cybersecurity. 2014. Disponível em: http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

[37] E-ISAC. Analysis of the cyber attack on the Ukrainian power grid. Disponível em: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[38] Reuters. Ukraine to probe suspected Russian cyber attack on grid. Disponível em: http://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UE0ZZ20151231

[39] Reuters. Ukraine points finger at Russian security services in recent cyber attack. Disponível em: 5https://www.reuters.com/article/us-cyber-attack-ukraine-idUSKBN19M39P

[40] NY Times. Crimea in dark after power lines are blown up. Disponível em: https://www.nytimes.com/2015/11/23/world/europe/power-lines-to-crimea-are-blown-up-cutting-off-electricity.html

eletrônica, dentro do ciberespaço. O mero fato de que isto tenha ocorrido é uma demonstração prática de como os serviços de funcionamento básico do Estado estão se conectando cada vez mais ao ciberespaço, e este, consequentemente, se tornando uma zona de completo interesse estatal. O problema que as tecnologias contemporâneas estão apresentando aos governantes é de que as sociedades estão se tornando quase que completamente dependentes destas tecnologias, e estas tecnologias aparentam ter problemas de segurança quase que crônicos. A digitalização dos serviços básicos de um Estado é tanto um grande avanço como um desafio.

Neste cenário, os Estados começam a mostrar sua força dentro do ciberespaço, e criam o que agora chamamos de *cyberwarfare*, ou as capacidades cibernéticas de guerra de um determinado ator. Os desentendimentos entre ucranianos e russos e as consequências destes dentro do ciberespaço mostram que Moscou passou uma mensagem de que se a Crimeia poderia ficar sem luz, a Ucrânia ocidental não era diferente. No mundo cibernético, os Estados agora se posicionam em busca de seus interesses, assim como o fazem nas outras zonas de influência, e com a crescente interação e dependência da sociedade nestas tecnologias, os governos agora necessitam explorar e ampliar suas capacidades nesta nova zona, e ao que parece, quem sair na frente terá grande vantagem. Ainda mais, como demonstrado no caso iraniano, percebe-se que o desenvolvimento de capacidades como o *malware* chamado Stuxnet pode se tornar uma tendência entre os Estados-nações. A necessidade de ocupar os espaços no ciberespaço por parte dos governos em congruência com a dinâmica plataforma dos aparelhos eletrônicos criam situações perigosas até mesmo para os desenvolvedores de armas cibernéticas, mas a efetividade de alguma destas armas pode significar uma grandiosa vantagem em alguma situação de guerra. Contextualizando estes fatos, um tipo de ciberguerra parece ser uma questão de tempo, e de fato, seja para se defender ou para se sobressair, os Estados já começaram a se preparar para isto.

3 Operações estatais no ciberespaço: o *cyberwarfare* e as grandes potências

As características do ciberespaço nos fazem entender a realidade da plataforma: os Estados devem investir e explorar cada vez mais o ambiente para adquirir segurança e vantagens estratégicas. As interações interestatais dentro desta plataforma nos trazem um novo conceito: o *cyberwarfare*. O *cyberwarfare* é uma combinação das capacidades cibernéticas e as interações entre dois ou mais atores dentro do ciberespaço. As operações de informação de um determinado ator, por exemplo, um Estado-Nação, também se enquadram no tópico por estarem diretamente conectadas com as capacidades cibernéticas no mundo contemporâneo.

Levando em conta os fatos apresentados no primeiro capítulo, entende-se que os Estados agora agem constantemente dentro do ciberespaço, e para entendermos os efeitos destas ações nas relações internacionais, devemos entender como os Estados podem atuar e quais são os efeitos de suas operações. As atividades cibernéticas de inteligência se alternam entre operações internas de segurança nacional e ações externas, que podem ser consideradas de guerra. Neste capítulo dividiremos os dois tipos de ação estatal cibernética e observaremos as diversas maneiras que um Estado opera em ações de guerra cibernética. Além disto, observaremos como as grandes potências como os Estados Unidos, China e Rússia entendem o *cyberwarfare* e como tratam esta questão publicamente, também observando o cunho de suas ações no ciberespaço.

As revelações de Edward Snowden chocaram boa parte do mundo, e mais do que um importante passo rumo à transparência, revelaram-se algumas maneiras que o governo estadunidense tratava a questão da segurança nacional. A espionagem de seus próprios cidadãos através da internet e das ligações telefônicas mostrou que a tecnologia estava sendo utilizada para garantir o controle geral sobre a sociedade. Porém, os cidadãos americanos não são os únicos a serem espionados por seus governos: vários países como a Alemanha[41], Irã[42], China[43] e França[44] apresentaram técnicas similares de monitoramento. Tanto no ocidente quanto no oriente, países monitoram a atividade de seus cidadãos por diversas maneiras, como o combate ao crime, manutenção da segurança nacional e vantagens políticas. Como a internet demonstra

[41] Spiegel. Secret Links between Germany and the NSA. 2013. Disponível em: http://www.spiegel.de/international/world/german-intelligence-worked-closely-with-nsa-on-data-surveillance-a-912355.html

[42] Reuters. Chinese company helps Iran spy on its citizens. 2012. Disponível em: http://www.reuters.com/article/us-iran-telecoms/special-report-chinese-firm-helps-iran-spy-on-citizens-idUSBRE82L0B820120322

[43] CDT. The world of Official Espionage. 2013. Disponível em: http://chinadigitaltimes.net/2013/02/wiretapping-wars-the-world-of-official-espionage/

[44] RFI. Le Monde. French government accused of widespread spying. 2013. Disponível em: http://en.rfi.fr/france/20130705-french-government-accused-widespread-spying-its-own-citizens

as características citadas no primeiro capítulo, onde usuários desta podem agir livremente na plataforma, criam-se neste cenário possibilidades de um indivíduo ou grupo se esquivar da esfera da lei. Por exemplo, o *website* Silk Road, um *website* existente na *Deep Web*[45], vendia drogas abertamente e entregava em endereços domésticos dentro dos Estados Unidos.[46] Neste cenário, o monitoramento de cidadãos pode ser útil para a aplicação da lei. Claro, os governos utilizam a ferramenta de maneira exagerada, e acabam entrando na inconstitucionalidade em alguns casos.[47]

Muito das operações informacionais internas de um governo também passam pelo controle das informações que chegam até seus cidadãos e as que saem para o mundo externo. Isto é claro no caso chinês. O Grande Firewall da China, termo em analogia à Grande Muralha da China, é uma camada de proteção cibernética criada pelos legisladores chineses em combinação com suas capacidades técnicas e novas tecnologias para regular e controlar a internet doméstica. Para os ocidentais, isto é uma clara censura à internet, e o esforço envolve o bloqueio a alguns sites estrangeiros e controle dos dados que saem para fora do país. Atividades que podem parecer triviais no ocidente, como uma busca no Google ou um perfil no Facebook, são alguns dos componentes da internet que são bloqueados em toda a China.

Na internet chinesa, uma série de medidas de segurança cibernética são aplicadas para controlar que tipo de informação entra e sai dos computadores chineses.[48] O bloqueio de endereços de IP, redirecionamento dos usuários para outros websites, e até mesmo a intrusão em conversas privadas são algumas das armas do firewall chinês, que afeta os 700 milhões de chineses conectados à internet.[49] Se considerarmos os dados da Internet Live Stats, de 3 bilhões de usuários para a internet, cerca de 1/4 da internet vive atrás do grande firewall chinês.

Uma boa parte dos objetivos específicos de Pequim passa por fortalecer as empresas domésticas ao dificultar o acesso aos produtos internacionais.[50] Grandes marcas internacionais ocidentais enfrentam dificuldades para adentrar o mercado chinês, e as regulamentações implementadas pela China em sua internet são mais uma barreira para a inserção no mercado.

---

[45] Deep Web: Conceito de parte da internet "escondida", somente acessível através de protocolos de segurança, contendo dentro dela uma série de informações variadas, incluindo de cunho ilegal.

[46] Forbes. End of the Silk Road. 2013. Disponível em: https://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/

[47] The Guardian. NSA mass surveillance ruled illegal by Federal Court. 2013. Disponível em: https://www.theguardian.com/us-news/2015/may/07/nsa-phone-records-program-illegal-court

[48] Harvard. Empirical Analysis of Internet Filtering in China. 2003. Disponível em: https://cyber.harvard.edu/filtering/china/

[49] TechInAsia. China now has 731 million internet users. 2017. Disponível em: https://www.techinasia.com/china-731-million-internet-users-end-2016

[50] BI. China bans Uber. 2015. Disponível em: http://www.businessinsider.com/uber-china-ban-2015-1

Primeiramente, as companhias domésticas chinesas ganham força, e as ocidentais sofrem com bloqueios e limitações impostas. De fato, a China trata publicamente a internet como parte de seu território, e o conceito de soberania na internet é firmemente aplicado. Não somente como um modelo de desenvolvimento das companhias chinesas e dando vantagens a estas através da legislação, Pequim também monitora as informações políticas para que as opiniões e valores ocidentais não se insiram na população. Na verdade, grandes *websites* como o Google e o Wikipedia são bloqueados na China, e em geral, as autoridades e empresários sempre apresentam uma alternativa aos serviços. Por exemplo, segundo o jornal The Independent, a China está lançando sua própria versão do Wikipedia, e só o partido comunista, que está no poder, pode contribuir para as informações que ali constarem.[51] Ainda que este seja um processo em andamento, empresas como Alibaba, de exportação e Baidu, de buscas e segurança online, se apresentam como realidades e fortes concorrentes aos serviços ocidentais. Pequim utiliza, com sucesso, a internet em seu favor.

A China nos últimos anos abraçou o mercado internacional, mas ainda se mostra extremamente desfavorável a qualquer tipo de intervenção política ocidental em suas questões internas. O seu *firewall* e projeto de monitoramento e censura servem para que mesmo sendo um país extremamente conectado ao mundo através do comércio, seus cidadãos sejam limitados ao tipo de informação que podem obter e disseminar. O *firewall* é contornável através de algumas especifidades, como por exemplo, a utilização de um VPN (*Virtual Private Network*, em inglês), que permite driblar bloqueios como este, porém as autoridades chinesas sabem disto. E mais: Para as autoridades chinesas, a elite, que sabe utilizar um VPN, por exemplo, pode muito bem acessar a internet global, desde que isto não afete a grande massa populacional. O programa chinês de monitoramento e censura é uma clara demonstração de como um Estado pode manipular o ciberespaço para seu próprio bem, e ainda nos demonstra algo diferente: a censura em ação. Enquanto que o sistema de monitoramento global revelado por Edward Snowden se provou ser muito amplo, devemos entender que existe uma grande diferença entre monitoramento e censura. Ao contrário do governo americano, o governo chinês controla deliberadamente as ações em seu território, e ainda promove isto publicamente através do manto da soberania.

Este tipo de comportamento demonstra como as operações informacionais internas no ciberespaço são efetuadas, e essencialmente, como são ferramentas importantes para a

[51] The Independent. 2017. Disponível em: http://www.independent.co.uk/news/world/asia/china-wikipedia-chinese-version-government-no-public-authors-contributions-communist-party-line-a7717861.html

manutenção do projeto de poder estatal e se provam ser cada dia mais úteis para os governos. Ainda que em níveis diferenciados, os governos, em geral, observam (e em alguns casos controlam) as ações de usuários na internet e se preparam para agir ou reagir de acordo.

3.1 Cyberguerra

Meados de 2005, Washington DC, Estados Unidos. Autoridades estadunidenses, quando questionadas, admitem a existência de uma investigação federal para recentes tentativas de intrusão em sistemas computadorizados norte-americanas, provenientes de território chinês. O que hoje é conhecida como a operação Titan Rain durou cerca de três anos e foi classificada pelas autoridades federais americanas como uma operação estrangeira coordenada que tinha como alvos sistemas computacionais de grande importância.[52] Entre os alvos afetados, computadores da NASA, FBI e até mesmo de sistemas militares de defesa. Ainda segundo as autoridades, os invasores mantinham persistentemente as ações e pareciam armazenar todas as informações em servidores externos antes de se desconectarem sem deixar trilhas. O analista de segurança Shawn Carpenter, que na época era um contratado do governo americano, afirmou que após um longo processo de busca, encontrou traços que levavam as atividades de invasão até a sua origem: Guangdong, na China.[53] Para Carpenter, os invasores, ou cyberespiões, como os chamam, agiam de maneira profissional ao não cometerem um sequer erro e deixavam claro que tinham alvos muito bem definidos, e a revista TIME, na época, deixou claro que autoridades americanas acreditavam que o governo chinês estava por trás destas ações.

Pequim jamais admitiu qualquer envolvimento com os fatos, mas os americanos acreditam até hoje que a operação Titan Rain foi uma operação estatal chinesa. As informações que os *hackers* buscavam obter eram de cunho militar ou sempre informações técnicas que poderiam revelar segredos de engenharia, por exemplo. Este fator, por si só, nos demonstra a realidade: Uma intrusão estrangeira em sistemas internos para obter informação privilegiada ou segredos estatais.

Se a China busca ampliar seu grande *firewall*, aparentemente também busca efetuar ações agressivas no ciberespaço. Enquanto que securitiza sua internet doméstica, o Partido Comunista investe em ações de ciberespionagem, como a operação Titan Rain, para atingir

[52] Testimony of Larry Wortzel. Cyberespionage and the theft of US intellectual property. 2013. Disponível em: http://docs.house.gov/meetings/IF/IF02/20130709/101104/HHRG-113-IF02-Wstate-WortzelL-20130709-U1.pdf

[53] Time Magazine. 2005. Operation Titan Rain. Disponível em: https://courses.cs.washington.edu/courses/csep590/05au/readings/titan.rain.htm

objetivos estratégicos. Se realizarmos uma analogia, as ações da operação Titan Rain nada mais são do que atos de guerra. A complexa relação entre a atribuição dos fatos e a comprovação desta atribuição no ciberespaço permite que, aos olhos do mundo, jamais haja um grande culpado pelas invasões aos sistemas americanos neste caso, mas os governantes sabem que agora, mais do que nunca, precisam se preparar para a ciberguerra. Os chineses, neste caso, entenderam que seria viável operacionalizar uma ação de espionagem dentro do ciberespaço, o que se provou como uma alternativa efetiva para Pequim. Além da incessante busca pela informação interna promovida por estes atores em busca de plena segurança e controle, os Estados-Nações agora buscam efetivar ações contra outros atores, neste caso, outro Estado-Nação, seja por motivo de auto-defesa ou para atingir algum objetivo estratégico. De fato, a guerra informacional, que é uma parte da guerra cibernética, começou, e necessitamos entender como e em que direção ela pode evoluir.

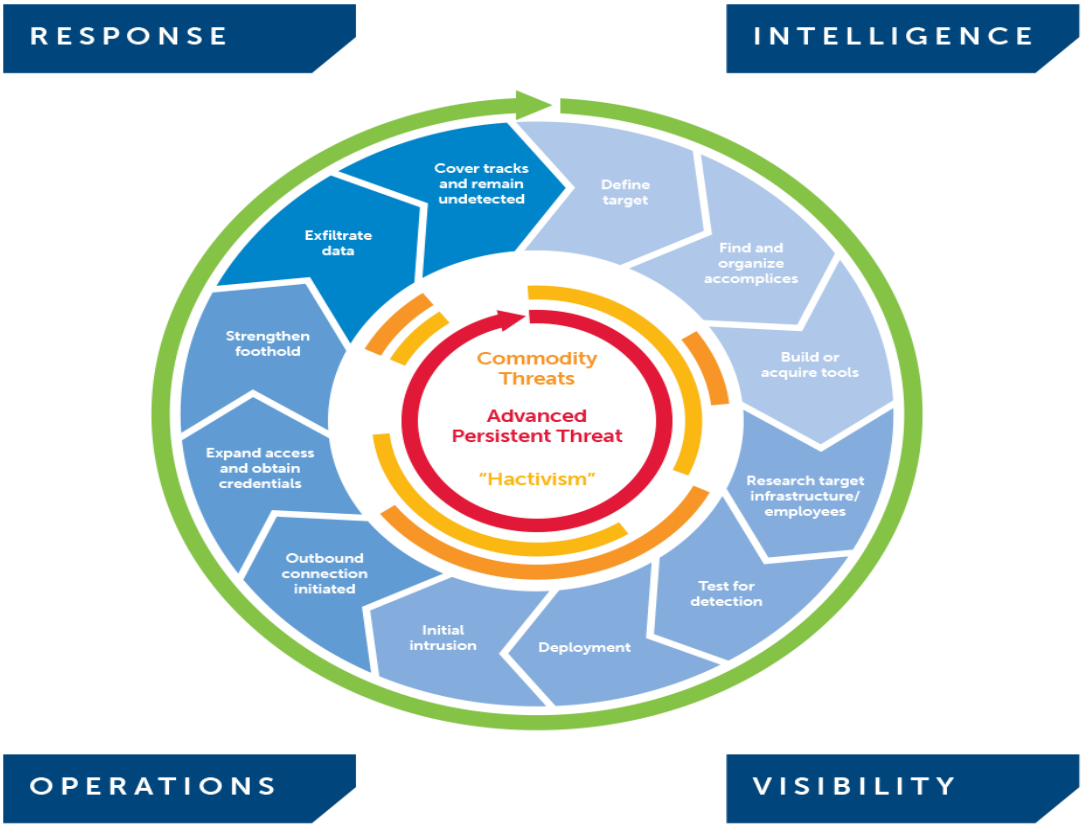
A operação Titan Rain é compreendida pela comunidade de inteligência não como uma simples ação ou operação de intrusão comum, mas sim como uma chamada APT, ou *Advanced Persistent Threat*, em inglês. Uma "ameaça persistente avançada" é um termo relativamente novo para classificar um tipo de ataque cibernético que envolve a intrusão aos sistemas computadorizados e acesso à informações privilegiadas por um longo período de tempo. Uma APT não é uma ação comum de usuários na internet, sendo que um dos principais pontos da ameaça é o fato de que o alvo sempre é específico, com alvos e objetivos bem definidos.

Em geral, um vírus malicioso é programado para que o autor usufrua de acesso a uma rede, e esta ação singular está muito relacionada a cibercriminosos solitários ou membro de pequenos grupos de ação. Os alvos são pré-determinados e generalizados, e as ações do código malicioso, gerais. Já nas APTs podemos observar um ciclo de ações específicas, onde o alvo é muito bem definido e as vulnerabilidades exploradas pelas ferramentas são específicas para determinada falha ou *bug* encontrado pelos *hackers*. As ferramentas utilizadas por estes atores variam entre *malwares*, *spywares*, injeções de SQL e afins.

Um estudo da Secureworks, companhia de segurança cibernética da Dell, mostra o funcionamento cíclico e a organização das ações de uma APT:[54]

[54] Secureworks. Advanced Persistent Threats. Disponível em: https://www.secureworks.com/blog/advanced-persistent-threats-apt-a

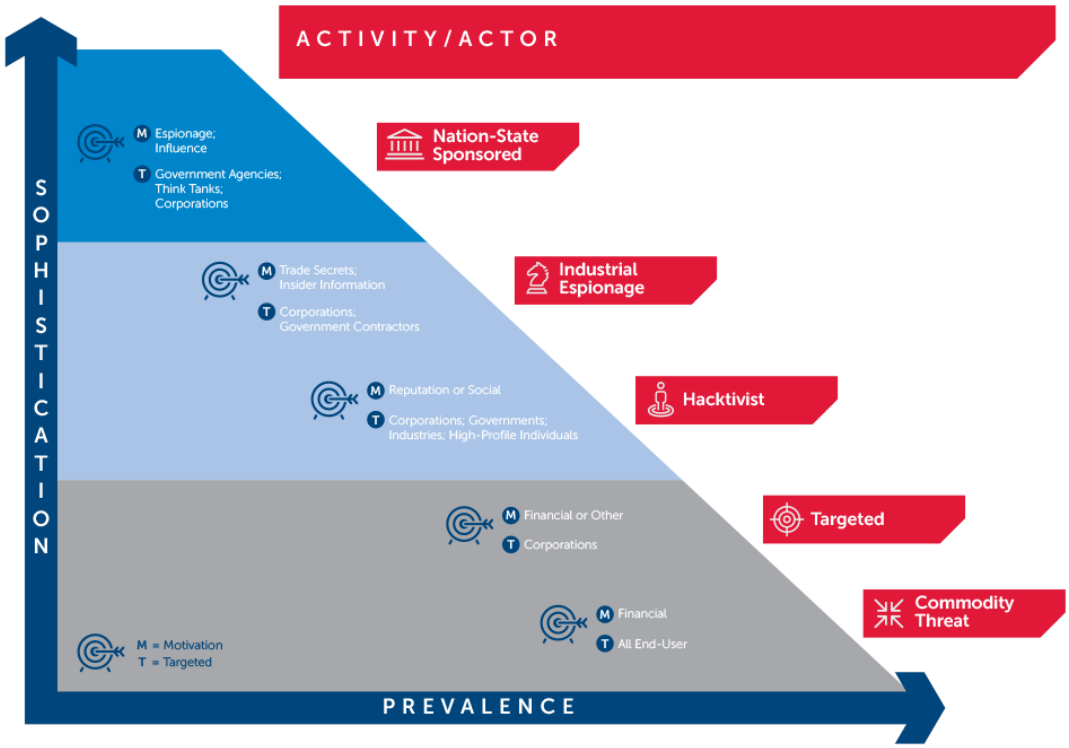
Figura 1 – Ciclo das APTs



Fonte: Secureworks. 2017. s/p.

Podemos observar um alto investimento como sendo um requerimento para que uma APT entre em ação. O nível de sofisticação, persistência, capacidade e investimento destas ações são extremamente altos, e analistas de segurança entendem que ações como esta são, em geral, proporcionadas por atores poderosos. Estados-Nações, organizações criminosas internacionais, grandes corporações e organizações terroristas podem estar por trás deste tipo de movimentação no ciberespaço. Compreende-se que diferentes atores tenham diferentes objetivos, mas uma padronização é observada pelos analistas da SecureWorks, como no gráfico a seguir:

Figura 2 – Relação ator/atividade



Fonte: Secureworks. 2017. s/p.

É possível observar que os alvos de espionagem no caso Titan Rain foram agências governamentais, e a capacidade para que estas ações fossem efetivas fazem com que os dedos sejam todos apontados à Pequim. De fato, uma APT é uma operação de espionagem utilizada por Estados-Nações para adquirirem informações preciosas para atuar no cenário internacional, e o caso da operação Titan Rain mostra um alto nível de sofisticação dos chineses no ciberespaço e como Pequim operacionaliza uma arma cibernética.

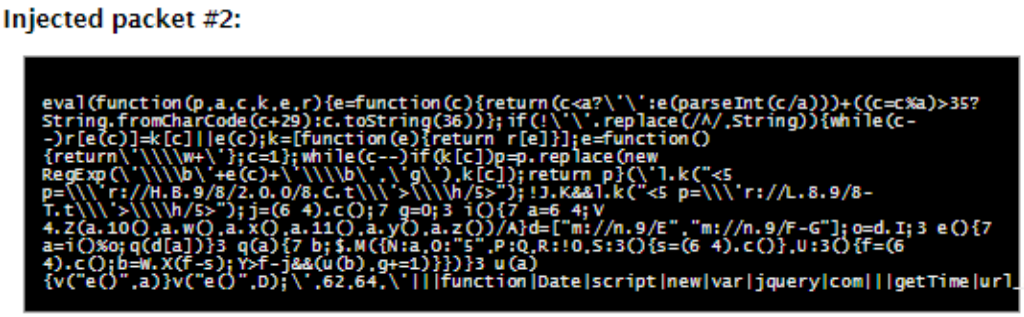
Se as ameaças persistentes avançadas são uma poderosa arma para reter ou obter informações, devemos entender que as capacidades cibernéticas de um ator estatal como a China não se limitam a monitorar informações. Em 2015, por diversas vezes, o *website* GitHub.com foi vítima de um ataque DDoS.[55] DDoS é a sigla em inglês para Distributed Denial of Service, ou um ataque de negação de serviço distribuido, e é o termo que ganhou fama no Brasil recentemente pelas ações de *hackers* contra sites governamentais.[56] O ataque de negação de serviço consiste de quando um servidor, onde os *websites* ficam armazenados, por exemplo,

[55] GitHub. GitHub under large scale DDoS attack. 2015. Disponível em: https://github.com/blog/1981-large-scale-ddos-attack-on-github-com
[56] G1. Ataque hacker ao Planalto. 2011. Disponível em: http://g1.globo.com/tecnologia/noticia/2011/06/ataque-hacker-foi-o-maior-ja-sofrido-por-sites-do-governo-na-internet.html

é maciçamente bombardeado por uma série de usuários com velocidade para sobrecarregar o sistema, e assim causar o desligamento ou provocar grande lentidão. Por muitas vezes, os *hackers* utilizam de computadores de terceiros, infectados, para realizar as ações, os conhecidos como "zumbis".[57]

O GitHub é uma plataforma onde desenvolvedores podem compartilhar projetos entre si, e é bastante utilizada para, por exemplo, compartilhar conteúdo proibido em determinados territórios. A companhia de monitoramento e segurança de rede Netresec realizou uma análise dos ataques DDoS nos servidores do GitHub e chegou a algumas conclusões.[58] Primeiramente, identificou-se que os alvos dos ataques eram duas páginas do GitHub que levavam ao New York Times em chinês e a um blog de notícias de fontes ocidentais em chinês, que podiam atravessar o *firewall* da China. O chamado ataque DDoS do Homem-ao-lado partiu de território chinês e infectava computadores fora da China que acessavam serviços chineses, como uma página do Baidu. Estes computadores infectados então agiam como zumbis, sobrecarregando os servidores do GitHub. O código malicioso pode ser visto abaixo:

Figura 3 – Código malicioso



Fonte: NetResec. 2016. s/p.

A complexa combinação de letras e números se traduz em uma infecção de um sistema desavisado partindo de uma injeção de código malicioso. No caso do ataque ao GitHub, os analistas de segurança concluiram que a injeção de código partiu de um JavaScript em um *website* que continha propagandas do Baidu, muito como o Google opera o Google Ads.[59] Depois de infectados, os usuários, muitas vezes sem perceber, incessantemente tentavam se conectar ao *website* do GitHub, causando sobrecarregamento e o desligamento do servidor. De

[57] TechTarget. Zombies. Disponível em: http://searchmidmarketsecurity.techtarget.com/definition/zombie
[58] NetResec. China's Man-on-the-Side attack on GitHub. Disponível em: http://www.netresec.com/?page=Blog&month=2015-03&post=China%27s-Man-on-the-Side-Attack-on-GitHub
[59] Forbes. How Google Ads works. 2014. Disponível em: https://www.forbes.com/sites/quora/2014/08/15/how-exactly-does-google-adwords-work

fato, analistas da NetResec contraíram o vírus, em caráter de teste, simplesmente por entrar em alguns *websites* chineses.

O fato de esta situação ser viabilizada pela utilização do mecanismo do Baidu, uma companhia chinesa, em usuários estrangeiros, nos mostra muito. Os chineses, neste caso, utilizaram o aparato cibernético que possuem para atingir um determinado objetivo. O *website* do GitHub é uma importante ferramenta para se driblar o bloqueio do *firewall* chinês, e um ataque tão específico aos canais de propagação de informação ocidental demonstra a existência de grande envolvimento de Pequim na questão. Essencialmente, os chineses parecem utilizar do aparato cibernético para alcançar alguns objetivos no cenário internacional. O Grande *Firewall* da China, e todo o projeto que o envolve, é muito mais do que apenas uma ferramenta de controle de informações. É, além disto, uma arma de guerra.

Os computadores zumbis não são a única arma automatizada dentro de um arsenal cibernético. Um recente estudo da FGV apresenta uma análise sobre a interferência de robôs, os famosos *bots*, no debate político público no Brasil, assim como seus riscos à democracia e ao processo eleitoral de 2018.[60] Os pesquisadores da FGV apresentam um interessante panorama, que nos faz melhor entender a questão da ação de *bots* em situações políticas. Como é apresentado na análise, e como argumentamos anteriormente aqui, a internet é utilizada como importante plataforma dentro da sociedade, e as redes sociais significam muito para a interação humana. Na era da informação, o fácil acesso à rede mundial de computadores se traduziu em uma ampla capacidade de expressão de opinião, fortalecendo o processo democrático mundo afora. Neste cenário, porém, pela natureza da internet, a quantidade de informações de fácil acesso na rede cresce rapidamente, abrindo assim espaço para discursos mentirosos e fatos irreais. As chamadas "*fake news*", que hoje são tema recorrente nos discursos de Donald Trump em ataques à parte da mídia norte-americana, se tornam uma arma a ser utilizada por um ator político para difundir uma mensagem falsa que pode beneficiá-los ou simplesmente denegrir a imagem da oposição, ou inimigo político.[61]

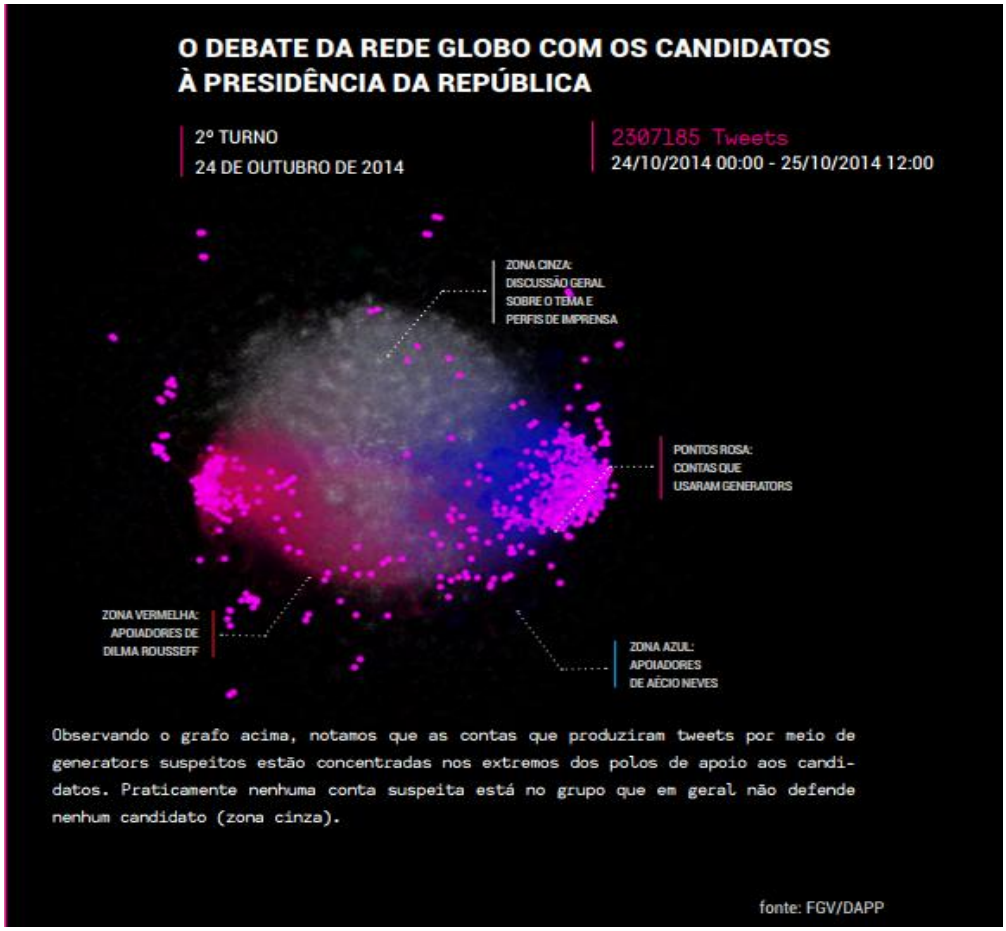
Os *bots* podem ser "contas em redes sociais controladas por *software* se fazendo passar por seres humanos", segundo a FGV. Os robôs são contas confeccionadas para simular um humano normal, a fim de influenciar a sociedade real, e podem partir de um servidor ou partir de uma máquina infectada. De fato, os *bots* podem ter papel importante na difusão de uma

[60] FGV. DAPP. Robôs, redes sociais e política no Brasil. 2017. Disponível em: http://dapp.fgv.br/wp-content/uploads/2017/08/Robos-redes-sociais-politica-fgv-dapp.pdf

[61] CNBC. Trump to CNN Reporter: You are fake news. 2017. Disponível em: https://www.cnbc.com/video/2017/01/11/trump-to-cnn-reporter-you-are-fake-news.html

mensagem política qualquer, já que boa parte da população consome notícias através da internet. Segundo o estudo, cerca de 20% das interações no Twitter foram iniciadas por robôs na campanha presidencial brasileira de 2014, assim fomentando e direcionando boa parte do debate público no país todo. Ainda, o estudo da FGV apresenta um gráfico mostrando como os *bots* no twitter brasileiro agiam na época:

Figura 4 – Bots no Brasil



Fonte: FGV/DAPP. 2017. P. 14

O caso brasileiro demonstra uma realidade global: As redes sociais, e a internet como um todo, são fonte primária de informação, construção de pensamento e organização política nos dias atuais. Assim sendo, a capacitação de ação efetiva dentro destas esferas de influência é essencial para obter qualquer tipo de vantagem estratégica que determinado ator desejar. A disseminação de notícias falsas é algo complexo, que afeta profundamente o processo democrático e pode causar graves depressões ideológicas dentro de uma sociedade. Ainda, ao observarmos o gráfico, analisa-se que os *bots* atuam nos extremos ideológicos dos dois candidatos mais populares, o que pode amplificar o campo de ação política de discursos mais extremos do que a sociedade de fato deseja. No caso brasileiro, isto pode se traduzir na recente

popularidade de Jair Bolsonaro, que acumula cada vez mais seguidores nas redes sociais e no Brasil afora. A ascensão de Bolsonaro envolve vários fatores, mas a polarização política no anticlímax político em Brasilia também passa pela atuação de *bots* e na discussão política nas redes sociais e na internet como um todo.

Hoje, nos Estados Unidos, por exemplo, dois terços dos adultos americanos utilizam de mídias sociais conectadas a redes sociais para obter informações, como Twitter e Facebook. Na América de Donald Trump, os "*fake news*" agora são termo recorrente, normalmente quando o presidente se defende de acusações, como as de que ele teve ajuda dos russos para vencer as eleições.[62] [63] De fato, o FBI afirmou que a Rússia utilizou de *bots* para divulgar e propagar notícias falsas para interferir na eleição presidencial norte-americana de 2016.[64] Trump, em resposta, passou a utilizar o termo "*fake news*" para a mídia convencional que divulgava as informações e condenavam o presidente, de maneira incessante. Com intervenção estrangeira ou não, as redes sociais tiveram grande papel nas eleições de 2016, como não poderia deixar de ser dada a nova realidade social humana.[65]

A utilização de *bots* para atingir determinados objetivos não é exclusividade de um grupo político nacional brasileiro, e os próprios pesquisadores da FGV, sobre isto afirmam:

> Ao identificarmos robôs operando para um campo, porém não queremos dizer que os atores políticos e públicos ali situados sejam responsáveis diretos pelos robôs a seu favor. Diversos grupos de interesse podem estar fazendo uso desse tipo de recurso de disseminação de informações. Na verdade, lato sensu, há robôs até operando do exterior. Isso inclusive enseja a reflexão de manipulação não só interna, mas também para além dos campos políticos nacionais, sugerindo a hipótese da possibilidade de até mesmo outros atores, estranhos ao quadro nacional, operarem nas redes esses mecanismos. (FGV, 2017, p. 9)

Em verdade, em um mundo cada vez mais conectado, grupos estrangeiros, incluindo outros Estados, podem estar por trás de ações envolvendo *bots* em redes sociais para atingir algum objetivo na discussão pública de determinado país. Em meio a acusações de interferência nas eleições americanas, a Rússia pareceu entender a funcionabilidade dos *bots* para divulgar uma mensagem desejada. Enquanto ainda são alvos de acusações quase que diariamente por

---

[62] Reuters. Two-thirds of American adults get news from social media. 2017. Disponível em: https://www.reuters.com/article/us-usa-internet-socialmedia/two-thirds-of-american-adults-get-news-from-social-media-survey-idUSKCN1BJ2A8

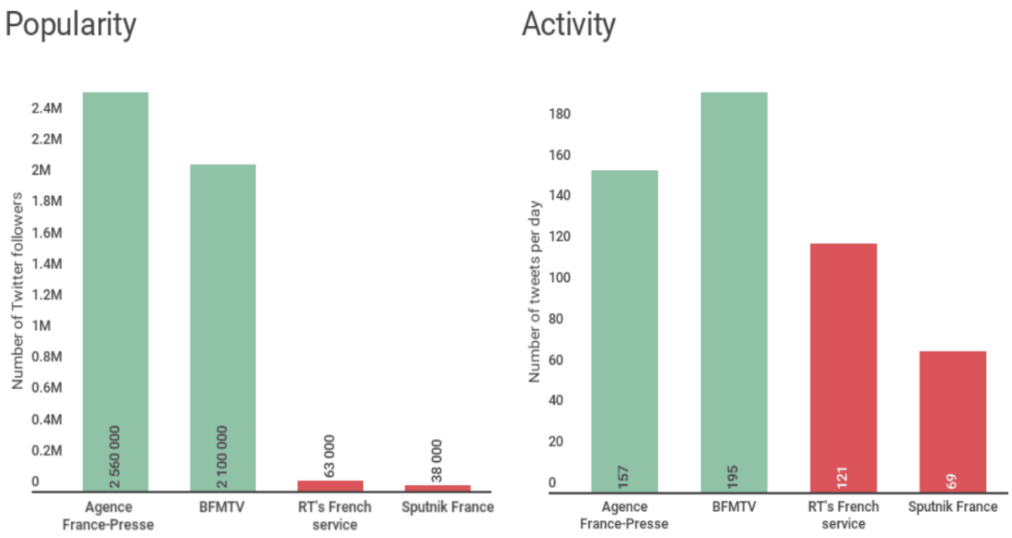
[63] Reuters. Russia-Trump campaign collusion an open issue. 2017. Disponível em: https://www.reuters.com/article/us-usa-trump-russia-senate-collusion/russia-trump-campaign-collusion-an-open-issue-u-s-senate-panel-chiefs-idUSKBN1C92G3

[64] NY Times. FBI. The fake americans. 2017. Disponível em: https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html

[65] HuffingtonPost. Social media and the 2016 presidential election. 2017. Disponível em: https://www.huffingtonpost.com/r-kay-green/the-game-changer-social-m_b_8568432.html

parte de grupos dentro dos Estados Unidos, um interessante estudo da Digital Forensic Research Lab mostra como os russos trataram a informação durante as eleições presidenciais francesas de 2017.[66] O estudo indica que entre os seguidores da gigante de mídia russa RT e do jornal Sputnik, no Twitter, estavam em sua maioria apoiadores de Marine Le Pen e suas políticas, opositores de Emmanuel Macron, apoiadores da Rússia e *bots* automatizados. Os jornais russos, RT e Sputnik, analisados neste estudo, são de alcance global, e o cunho de suas informações é, em geral, pró-Kremlin.[67] Na França, os seguidores destas mídias russas em plataformas como o Twitter estão em número muito menor do que de algumas outras agências, como a francesa Agence France-Presse. Ainda assim, nas eleições de 2017, a atividade nas redes sociais franco-russas foi grandiosa:

Figura 5 – Popularidade e atividade no Twitter francês



Fonte: DFR Lab. 2017. s/p.

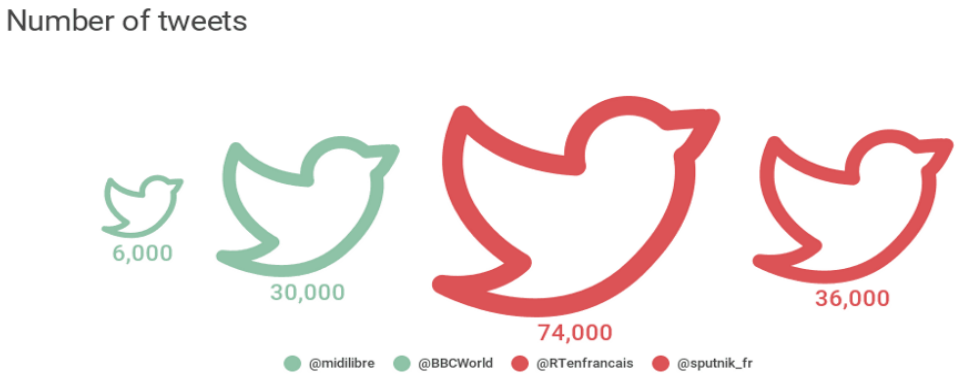
O gráfico é claro: Mesmo sendo extremamente menos popular do que agências consagradas na França, o serviço francês da mídia russa teve uma atividade quase que igual a redes que afetam muito mais pessoas. O efeito que isto aparenta ter é uma maior difusão das ideias ali apresentadas por estas mídias, dando uma impressão de um número maior de defensores de determinada ideia. Ainda, temos de entender que não somente as atividades das mídias russas são responsáveis pela disseminação de notícias. Os usuários em uma rede social,

[66] DFR Lab. The Kremlin's Audience in France. 2017. Disponível em: https://medium.com/dfrlab/the-kremlins-audience-in-france-884a80515f8b

[67] Folha de S. Paulo. RT: Noticias ou Propaganda? 2017. Disponível em: http://www1.folha.uol.com.br/mundo/2017/03/1865017-emissora-russa-rt-e-agencias-de-noticias-ou-propaganda-do-kremlin.shtml

como o Twitter, e suas reações ao conteúdo publicado, como compartilhar ou repostar, é que ampliam e difusão a mensagem passada por um canal de notícias. É neste cenário que os *bots* podem agir, já que se passam por e ainda superamocs humanos em relação à atividade online, devido ao processo automatizado:

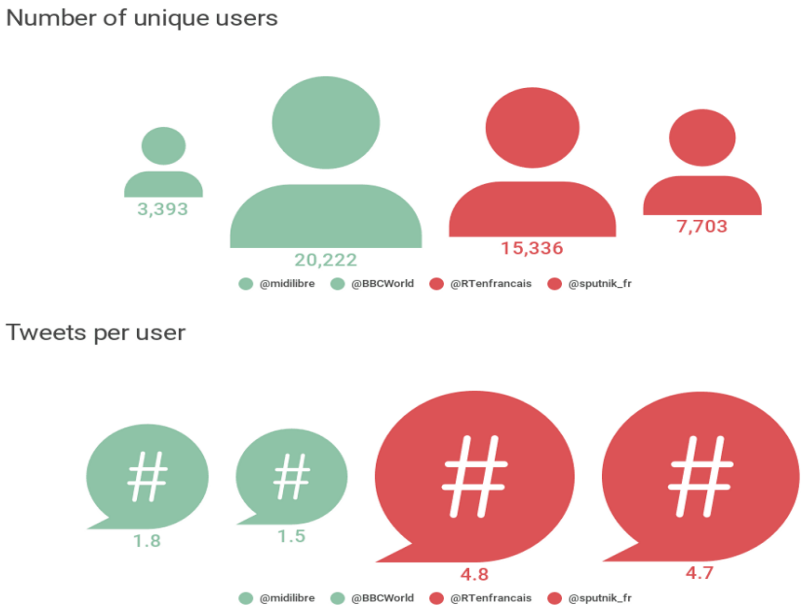
Figura 6 – Tweets da BBC/RT/Sputnik



Fonte: DFR Lab. 2017. s/p.

Observa-se a grande quantidade de *tweets* que interagiram com as contas do @RTFrancais e do @Sputnik_fr no Twitter. Com um número muito menor de seguidores, como visto no primeiro gráfico do estudo, os usuários conectados aos serviços russos na França postaram mais do que o dobro de vezes do que os milhões de seguidores do serviço da BBC. A indicação de *bots* é clara:

Figura 7 – Usuários únicos no Twitter francês



Fonte: DFR Lab. 2017. s/p.

No gráfico, pode-se observar que o número de usuários únicos a realizarem estas ações é menor entre os seguidores do RT e Sputnik. Ainda, o número de *tweets* por usuário quase chega a 5, em comparação com o 1,5 da BBC. O que pode entender-se disto é uma clara automatização dos serviços de divulgação, principalmente por parte dos usuários conectados aos serviços de mídia russa na França. Ainda que nem todos sejam *bots*, é muito considerável o número e a intensidade de interações para que seja divulgada uma mensagem.

A atividade de *bots* na França é um claro exemplo de como o ciberespaço pode ser utilizado para melhor difundir notícias que sejam de determinado interesse para um ator. No caso dos russos, que tem óbvia conexão com Marine Le Pen, incluindo financeiras, já que esta repetidamente obteu empréstimos de bancos russos, o Twitter e as outras redes sociais podem ser interessantes plataformas para apoiar as ideias que interessam.[68] [69] O caso dos *bots* automatizados promovendo notícias prejudiciais à Macron, e beneficiais à Le Pen mostram como os *bots* e o ciberespaço também são partes de uma guerra silenciosa: a guerra da informação. Mesmo que a relação entre o Kremlin e os serviços midiáticos não seja confirmada, as ações demonstram clara intenção de ao menos um poderoso grupo na Rússia em atingir determinada camada de eleitores franceses.

[68] Folha de S. Paulo. Putin se reúne com Le Pen. 2017. Disponível em: http://www1.folha.uol.com.br/mundo/2017/03/1869375-em-moscou-putin-se-reune-com-a-ultradireitista-francesa-marine-le-pen.shtml

[69] BBC. Marine Le Pen: Who's funding France's far-right? 2016. Disponível em: http://www.bbc.com/news/world-europe-39478066

3.2 As capacidades cibernéticas

Observando os exemplos aqui citados, podemos notar como se operacionalizam algumas das interações no ciberespaço, e como tomaria forma uma guerra virtual. No caso dos chineses, observa-se que o ciberespaço é essencial para a manutenção da segurança nacional, e ali vai se criando um novo paradigma sobre o que é e como deve ser usada a internet. Além disso, os chineses operacionalizam ações mais invasivas no ciberespaço, como em atividades agressivas no ciberespaço, com intrusões de moral questionável ao pensamento democrático ocidental. No caso brasileiro, observa-se como grupos políticos buscam influenciar a opinião pública com medidas sutis, como a distorção e divulgação em massa de informação de cunho político, ou seja, que afetam diretamente questões partidárias e de grande importância pública, que agem na simpatização gradual de parte da população à determinada ideologia ou figura pública. De fato, a sutileza desta operação de *bots* no Twitter e outras redes sociais online é que a faz tão perigosa, por afetar o pensamento dos indivíduos com informações falsas e ainda inchar movimentos não tão populares, afetando gravemente o processo democrático real.

Para Martin Libicki, este processo de distorção de informações é parte essencial do processo de guerra no ciberespaço. Ele diz:[70]

> People impose nuclear weapons on others, but, as noted, there is no forced penetration in cyberspace. Hackers have little extant ability to create entry paths – only to exploit them. Information warfare, as noted, is strongly related to deception at one level or another [...] (LIBICKI, 2007, p. 39).[71]

O argumento de Libicki é o de que no ciberespaço, não existe entrada forçada, ou seja, invasões agressivas. Nas situações da era nuclear, e da tecnologia de guerra nuclear, a imposição de uma potência que detém uma bomba nuclear é grandiosa sobre as nações que não possuem a tecnologia, e a utilização da bomba pode matar milhares de pessoas, como em Hiroshima e Nagasaki, mais de sete décadas atrás.

Já na era da tecnologia da informação, a principal característica de capacidades de guerra informacional está relacionada à capacidade de fraudar ou enganar indivíduos e grupos. Na realidade, um *hacker* baseia boa parte de suas atividades em iludir, enganar e determinar o caminho de seu alvo, sendo que a engenharia social é essencial no processo da guerra

[70] LIBICKI, Martin. Conquest in Cyberspace: National Security and Information Warfare. Cambridge University Press, 2007.

[71] Nossa tradução: As pessoas impõem armas nucleares aos outros, mas, como observado, não há penetração forçada no ciberespaço. Os hackers têm pouca capacidade de criar caminhos de entrada - apenas para explorá-los. A guerra da informação, como observado, está fortemente relacionada ao engano em um nível ou outro

cibernética.[72] Ainda que seja realizada online, por exemplo, em emails, os *hackers* terão de se passar por alguém, ou enviar algum tipo de mensagem atrativa para que os usuários alvos possam interagir e contrair um vírus mais específico. Em geral, os *hackers* utilizarão de mensagens falsas, enganando os usuários, para que abram algum tipo de arquivo ou *website*, e assim se tornem controlados pelos *hackers*. Por vezes, alguns agentes podem agir físicamente, como é suspeitado que tenha ocorrido em Natanz, no Irã, mas a incidência dessas operações é menor.[73] De qualquer maneira, a utilização do processo de fraude de informação é parte essencial da guerra cibernética. Libicki (2007, p. 40) ainda afirma que a capacidade de ser enganado e de enganar parece ser inerente aos humanos e seus sistemas como um todo.

De fato, o entendimento de Libicki de que a guerra cibernética é diferente da guerra convencional é uma realidade pela própria natureza da plataforma. A rede mundial de computadores e seus sistemas interligados são basicamente feitos de informação e *hardware*. A principal afetada no processo de securitização desta rede só poderia ser a informação, que é crucial para a administração estatal hoje. Além disso, o investimento em *hardware* é algo dado, também. Assim sendo, o caso brasileiro é uma demonstração de como este processo é uma questão importantissima. No caso das eleições francesas, os russos agiram de forma sutil, porém passando uma forte mensagem. Marine Le Pen passou para o segundo turno, e claro, por vários outros fatores, mas o fato de que os russos focavam apoiar esta candidata em determinados momentos mostra a eficácia das operações, mesmo que de forma gradual. Mesmo que não eleita, a polarização e extremização do discurso político, duas características de Le Pen, se inflam e o processo político real também é ameaçado gradualmente. Ali, os russos mostraram que a informação, quando passada de determinada maneira, pode atrair seguidores e ampliar o espectro de influência de determinada figura ou ideologia. Nesta questão, que observaremos mais à frente, deve-se entender quem se beneficia desta situação. De fato, este tipo de operação parece ter seu maior benefício na questão de que pela sutileza, não atrai grandes prejuízos para o ator. Claro, a mesma tática pode ser utilizada contra este ator, porém, a relevância e eficiência são amplamente mutáveis neste tipo de operação. No caso da França, os russos puderam ampliar seu campo de atuação, enquanto que a um custo mínimo.

---

[72] SILVA, Narjara Bárbara Xavier; Engenharia social nas redes sociais online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. Revista Ibero-Americana de Ciência da Informação, [S.l.], v. 6, n. 2, mar. 2014. ISSN 1983-5213. Disponível em: <http://periodicos.unb.br/index.php/RICI/article/view/9222>. Acesso em: 12 out. 2017.

[73] C-NET. Stuxnet delivered on drive. 2012. Disponível em: https://www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/

No entanto, é aqui que percebemos a tal separação de dois tipos de atuação no ciberespaço, citados no início do capítulo. O caso brasileiro, o da França, e até mesmo o *firewall* chinês, nos mostram que o controle, distorção e divulgação de informação são armas poderosas em uma operação cibernética, mas o campo de atuação destas está mais limitado ao imaginário das pessoas que se traduz em efeitos no processo democrático de forma progressiva. Já nas situações como no Irã e na Ucrânia, onde houveram danos físicos consideráveis a estruturas essenciais para algum tipo de serviço, a atuação parece ser mais efetiva a curto prazo, porém é percebida como uma clara agressão e o fator da sutileza deixa de existir.

No caso da *grid* ucraniana, que vimos anteriormente, a ação invasiva no ciberespaço causou não somente confusão mental aos ucranianos, como também os deixou sem energia e sem notícias do que estava acontecendo. Sim, o processo de invasão do sistema elétrico ucraniano se deu por atividades de *hackers* que, como dito, adquiriram informações através da engenharia social para então controlar a rede, mas depois disto, realizaram ações agressivas com danos instantâneos ou semi-instantâneos. De fato, os ucranianos foram atingidos em um importante fator da convivência em sociedade contemporânea, a utilização da energia elétrica. Se realizarmos uma contextualização com a realidade das guerras convencionais, podemos entender que isto seria o equivalente a jogar uma bomba em um país.

Portanto, entende-se que atores internacionais, principalmente os governos de Estados-Nações, dão atenção especial para as capacidades de ciberguerra, até mesmo por precaução. Entendemos os tipos de ações que são realizadas no ciberespaço, e tanto as ações sutis quanto as ações mais agressivas podem ser extremamente prejudiciais para um ator, seja este um Estado, uma corporação, empresa ou algo do tipo. Em um mundo onde a informação é fonte de sucesso e dinheiro, além de um importante fator da administração pública para o Estado, existe a necessidade de se preparar para enfrentar os desafios que podem partir de atores com diversos interesses, estes atores sendo domésticos ou estranhos ao quadro nacional. Ainda mais, com o avanço e disseminação do ciberespaço, as informações não estão sozinhas na zona de atuação de atores dentro deste espaço, mas fazem parte de um grupo de plataformas que incluem, por exemplo, as *smart grids* elétricas conectadas e outras infraestruturas relacionadas à serviços essenciais para uma sociedade. Nestas infraestruturas e serviços, uma operação de ciberguerra pode inferir danos irreparáveis ou até mesmo custarem uma guerra. A dependência da infraestrutura governamental em serviços conectados ao ciberespaço criou, portanto, uma vasta zona de influência para atores nacionais e internacionais, assim sendo uma questão de segurança nacional para Estados-Nações.

Neste cenário, os governantes e outros atores interessados rapidamente partem para o investimento e inovação em uma área ainda muito não explorada, e em rápida mutação. Conforme o avanço técnológico surge mais rapidamente na sociedade, os Estados, priorizando sua segurança nacional e desenvolvimento econômico, rapidamente implementam mudanças em suas maneiras de agir e ferramentas a serem utilizadas. Por exemplo, ao modernizar um sistema de transporte conectando-o à internet. Além disso, agências de segurança nacional e espionagem trabalham para produzir códigos maliciosos mais eficientes e as indústrias sempre produzindo *hardware* mais potente. Para contextualizarmos este cenário com as relações internacionais, devemos entender o que e quais são as capacidades cibernéticas dos principais atores no sistema mundo. O poder digital é uma realidade, e em um mundo hiperconectado é uma necessidade mesmo que só para se defender de agentes hostis.

O poder cibernético, como apontado anteriormente, é uma realidade contemporânea. Dada a relevância da plataforma e dos avanços tecnológicos para a sociedade, o ciberespaço se apresenta como uma nova zona de influência e disputa por poder. Para Joseph Nye, o "ciberespaço não substituirá o espaço geográfico e não destruirá a soberania estatal, mas a difusão de poder no ciberespaço irá coexistir e complicar grandiosamente o que significa o exercício do poder nestas dimensões".[74] De fato, para entendermos como se dá o desenrolar das relações internacionais no ciberespaço, devemos compreender o conceito de poder neste espaço e como isto se reflete nas ações de importantes atores internacionais. Joseph Nye segue:

> Cyber power behavior rests upon a set of resources that relate to the creation, control and communication of electronic and computer based information -- infrastructure, networks, software, human skills. This includes the Internet of networked computers, but also intranets, cellular technologies and space based communications. Defined behaviorally, 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 (NYE, 2010. p. 4).[75]

[74] NYE, Joseph S. Cyber Power. Harvard Kennedy School. Belfer Center. 2010. Disponível em: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf

[75] Nossa tradução: O comportamento do poder cibernético recai sobre um conjunto de recursos relacionados à criação, controle e comunicação de informações eletrônicas e baseadas em computador - infra-estrutura, redes, software, habilidades humanas. Isso inclui a Internet de computadores em rede, mas também intranets, tecnologias celulares e comunicações espaciais. Definitivamente, o poder cibernético é a capacidade de obter resultados preferenciais através do uso dos recursos de informação interligados eletronicamente do domínio cibernético. Em uma definição amplamente utilizada, o poder cibernético é "a capacidade de usar o ciberespaço para criar vantagens e influenciar eventos em outros ambientes operacionais e em todos os instrumentos do poder". O poder cibernético pode ser usado para produzir resultados preferidos no ciberespaço ou pode usar instrumentos cibernéticos para produzir resultados preferidos em outros domínios fora do ciberespaço.

Para Nye, o conceito de poder muito passa pela capacidade de ter seus objetivos e vontades atendidos, seja através de coerção física (*hard power*) ou através de ações mais sutis, que afetam o psicológico de pessoas, grupos e nações (*soft power*). No poder cibernético, o conceito é aplicado e contextualizado para que o ciberespaço seja utilizado como um meio viabilizador de vantagens e objetivos de determinados atores. Ainda, como observamos nos capitulos anteriores, as ações no ciberespaço podem produzir um resultado dentro do ciberespaço, ou fora dele.

Como vimos no caso da *smart grid* ucraniana, uma ação originária do ciberespaço causou grandes danos fora deste ciberespaço, deixando milhares sem energia elétrica. Ao mesmo tempo, as ações de censura por parte dos chineses no ataque ao GitHub produziram efeitos poderosos, mas somente dentro do ciberespaço. Para entender melhor, Nye divide os tipos de ações no ciberespaço em *Hard Power* e *Soft Power*, na seguinte tabela:

Tabela 1 – Alvos de ataques cibernéticos

Alvos do poder cibernético	Intra ciberespaço	Extra ciberespaço
Instrumentos de informação	Hard: ataques DDoS Soft: Delinear normas e padrões	Hard: Ataque a sistemas SCADA (como smart grids) Soft: Campanha diplomática pública para alterar a opinião
Instrumentos físicos	Hard: controle governamental sobre companhias Soft: Infraestrutura para apoiar ativistas de direitos humanos	Hard: bombardear roteadores ou cortar cabos Soft: Protestos para envergonhar provedores cibernéticos

Fonte: Traduzido e adaptado de Joseph Nye. 2010. P. 7.

Para ele, as três faces do poder cibernético são essas. Primeiro, a indução de ação em outro ator, que pode tomar corpo em ações de *hard power* (ataques DDoS, inserção de malware, e emprisionamento de *bloggers*), assim como pode realizar ações de *soft power* (campanhas de publicidade com alvos específicos, para recrutar hackers, por exemplo, muito como se faz hoje no Estado Islâmico). A segunda face do poder cibernético é o controle de agenda, ou seja, minimizar as estratégias de determinado ator ao excluir a possibilidade destas existirem. Por exemplo, no caso do *firewall* chinês, se limita o campo de atuação política de possíveis forças opositoras. Este mesmo controle pode ser entendido como legítimo, se mascarado atrás de

regulamentações de software bem aceitas por determinado grupo ou sociedade. A terceira face para Nye é onde os atores desenham as preferências do outro ator para que nem se considere determinada estratégia deste outro ator. Por exemplo, a manipulação de informação e a distribuição massificada desta em operações estrangeiras podem ser uma operação *de soft power* extremamente eficiente para os russos, principalmente em uma época de crescente nacionalismo e conservadorismo na Europa.

A conceitualização de Nye é conveniente por nos demonstrar como funciona o poder cibernético e como são divididas as ações no campo teórico das relações internacionais. Como o ciberespaço é, como dito anteriormente, essencialmente informação, os atores deverão lidar da melhor maneira que considerarem com esta mesma informação, para então definir seu curso de ações. Um interessante fator do poder cibernético é que ele difere de conceitos mais antigos e bem compreendidos nas relações internacionais. O poder aéreo, ou o poder marítimo, se apresentam como questões bem estabelecidas no campo teórico e até mesmo no campo factível das relações internacionais, mas o poder cibernético recentemente começou a ser "testado" e implementado por diversos atores. Porém, o poder cibernético, mesmo sendo diferente e recente, não é algo que surgiu de outro mundo. Feito por humanos, o ciberespaço também tem algumas características parecidas com o espaço convencional, e o poder cibernético, portanto, também apresenta algumas características parecidas.

Por exemplo, é verdade, como propomos desde o início neste trabalho, que o ciberespaço abre campo para atuação de atores não-estatais, assim como cibercriminosos, organizações terroristas e afins. Ainda, é verdade que ações de um só indivíduo ou pequeno grupo bem capacitado podem ter efeitos grandiosos, e como coloca Nye, a difusão de poder no ciberespaço é muito maior do que no espaço aéreo ou marítimo, por exemplo. Porém, os Estados ainda seguem sendo os principais atores dentro do ciberespaço. Um dos motivos, por exemplo, é o simples fato de que o poder cibernético também precisa de recursos humanos, e quanto maiores os recursos humanos, maiores as operações no ciberespaço. Ainda, em um ambiente desenvolvido, onde hackers podem surgir e se especializar com mais facilidade, por exemplo, em um país onde o investimento na educação na área é grande, podem surgir atores mais capacitados e hábeis para agir no ciberespaço. Como bem coloca Aaron Brantly, um exército bem treinado é melhor que um não treinado, e o mesmo se aplica aos hackers que atuam no ciberespaço. Portanto, um Estado, com seus grandiosos recursos, permanece como o principal ator dentro desta plataforma. Para compreender melhor, Nye apresenta a seguinte tabela:

Tabela 2 – As faces do poder cibernético

As três faces do poder no ciberespaço
Face 1: (A induz B para que B faça o que B não faria inicialmente)
Hard power: ataques DDoS, inserção de malware, ataques a sistemas SCADA, prisão de ativistas e blogueiros
Soft power: campanha informacional para alterar as preferências de hackers, recrutamento de membros para organizações terroristas
Face 2: (Controle de agenda: A controla as opções estratégicas de B ao evitar que B acesse tais estratégias)
Hard power: firewalls, filtros, e pressão sobre companhias para controlar conteúdo
Soft power: controle de conteúdo através dos provedores de ISP, regras em domínios online, e padronização de software
Face 3: (A molda as preferências de B para que algumas estratégias nunca nem sejam consideradas)
Hard power: ameaças de punição para quem divulgar determinadas informações
Soft power: informação para criar preferências (exemplo: estimular o nacionalismo e "hackers patrióticos"), desenvolver formas de criar repulsa

Fonte: Traduzido e adaptado de Joseph Nye, 2010, p.15

Na tabela, Nye apresenta as características dos recursos cibernéticos de cada tipo de ator e também, suas vulnerabilidades. Fica claro que a superioridade estatal muito se baseia em seus recursos econômicos (para desenvolver infraestrutura, educação e propriedade intelectual, e controlar os mercados de ações), assim como em suas instituições legais como a constituição como base do poder estatal, sendo que o governo detém o poder de realizar operações físicas dentro de seu espaço territorial, como por exemplo, apreender hackers criminosos e atividades do tipo. Ainda, os governos são amplamente compreendidos como fonte de legitimidade, portanto, para Nye, podem produzir conteúdo de *soft power* factível e de qualidade.

Ainda, outros atores, mesmo que menos poderosos, detém grande capacidade de ação. No caso de organizações e redes, a flexibilidade das ações e a capacidade transnacional de atuação são importantes ferramentas de poder. Se pensarmos em individuais ou pequenos grupos, podemos observar que mesmo com menos recursos, as vantagens ainda são existentes devido ao baixo custo de uma ação cibernética, além da possibilidade de se esconder atrás da camada de anonimato da plataforma. De fato, Nye (2010, p.12) argumenta que apenas cinco porcento dos cibercriminosos em toda a história foram presos ou condenados.

Os dados parecem nos levar a crer que as atividades de indivíduos no ciberespaço compensam o risco. De fato, ao contextualizarmos isto com as relações internacionais, a

assimetria do poder cibernético é uma das questões mais importantes para se levar em conta no tópico. Um Estado extremamente inserido no ciberespaço, através de infraestrutura e processos administrativos, é também um grande alvo para diversos tipos de ações. Esta assimetria pode ser identificada ao compararmos as vulnerabilidades de um ator governamental com as de um ator individual como proposto por Nye. Os governos têm muito a perder em um cenário de guerra cibernética, e por isso estes atores individuais detém um certo poder.

Essencialmente, as vulnerabilidades de determinado ator acabam tendo um papel determinante para entendermos o seu poder cibernético. Para Ryan Maness, as vulnerabilidades dos atores possuem dois fatores importantes a serem levados em conta: sua capacidade de ciber defesa e sua ciber dependência. Como muito colocamos no primeiro capítulo, a ciber dependência é fruto da tendência de determinado ator estar extremamente conectado ao ciberespaço, por exemplo, como nos casos dos Estados Unidos, onde a infraestrutura está em parte conectada à internet. Enquanto que benéfico em algumas áreas, esta conectividade demasiada apresenta uma séria ameaça ao Estado no ciberespaço, o tornando mais vulnerável e portanto, menos poderoso em termos cibernéticos. Maness apresenta um *ranking* das capacidades cibernéticas entre grandes atores internacionais:

Tabela 3 – Capacidades cibernéticas estatais

State	Cyber-Offense	Cyber-Dependence	Cyber-Defense	Total Score
Iran	4	5	3	12
Great Britain	7	2	4	13
Germany	7	2	4	13
South Korea	6	4	4	14
North Korea	3	9	2	14
United States	9	2	4	15
Israel	8	3	4	15
China	6	4	6	16
Russia	7	3	7	17

Fonte: MANESS, Ryan. Políticas cibernéticas como fonte de poder. 2015. P. 9

Para ele, as capacidades cibernéticas ofensivas se baseiam em "quão avançado tecnologicamente é o Estado e a quantidade de recursos humanos bem preparados este detém". A ciber defesa é baseada na capacidade de as autoridades estatais têm em seu território de exercer o controle sobre as informações entrando e saindo da internet, como é o caso chinês. Na tabela, podemos observar que a ciber dependência é considerada ao inverso, e quanto mais conectada a infraestrutura de um país ao ciberespaço, menor a sua pontuação. Disto podemos

entender que por exemplo, em um país como a Coreia do Norte, onde o nível de conectividade de cidadãos e de sistemas governamentais de infraestrutura é mínimo, a ameaça de um ataque cibernético é muito menos relevante, e o investimento nas capacidades ofensivas é vantajoso pelo simples fato de o país poder se igualar a grandes potências militares a um custo e risco baixo.

Ainda, na tabela, nota-se como os países ocidentais tem uma capacidade de defesa menor do que os chineses e os russos. Muito deste fator pode ser explicado pela contextualização de Aaron Brantly, onde entende-se que a estrutura judicial e a regulamentação da internet e do ciberespaço são fatores essenciais na questão do poder cibernético. De fato, para se defender no ciberespaço, o Estado deve ter a capacidade de exercer sua autoridade jurisdicional que é comum ao ambiente convencional, mas uma incógnita para o ciberespaço. Na Rússia, as autoridades exercem grande controle sobre o fluxo de informações na internet, o que vem provando ser um impecilho para os legisladores em Washington. Portanto, as capacidades de defesa da China e Rússia, que não são democracias ocidentais, facilmente ultrapassam as capacidades de defesa das potências ocidentais, que se torna um fator de preocupação por estar sendo inviabilizada pela burocracia democrática.

No campo ofensivo, os Estados Unidos demonstram uma superioridade em relação aos demais. De fato, o desenvolvimento do Stuxnet, assim como a possível existência de grandes grupos de agentes de inteligência norte-americanos focados em ações no ciberespaço demonstram o poderio de Washington. É muito possível, portanto, que o ator com maior capacidade cibernética ofensiva seja Washington, mas o poder cibernético não é feito somente de capacidades ofensivas. A Rússia é a primeira colocada do ranking, sendo assim, o ator "mais perigoso" nas relações cibernéticas internacionais, nas palavras de Maness.

Em Moscou, o monitoramento da internet realizado pela FSB, assim como contar com o apoio de uma das maiores e mais avançadas empresas de segurança cibernética (Kaspersky) são fatores que colocam a Rússia como o Estado mais bem preparado defensivamente no ciberespaço. Ainda, a sua inserção relativamente baixa nas questões de dependência de infraestrutura em comparação à outras potências a tornam uma fortaleza digital. Maness argumenta que no campo das ações ofensivas, o nacionalismo e orgulho russo em combinação com a falta de empregos no setor tecnológico criam uma grande quantidade de comunidades de *hackers* nacionalistas, com "potencial para inflingir danos em Estados-Nações". A capacidade ofensiva da comunidade cibernética russa é, portanto, maciça, e se bem organizada, pode causar graves danos à outros atores, como veremos no próximo capítulo. De fato, para Nye, "as

habilidades de *hackers* de grupos criminosos podem tornar estes grupos aliados naturais de Estados-Nações que procuram aumentar suas capacidades enquanto rejeitam qualquer envolvimento em ciberataques" (apud NYE 2010, p. 12). Como é colocado por Nye, as características específicas do ciberespaço, onde a anonimidade é um fator comum, podem causar uma interessante convergência de interesses de diferentes atores. No caso russo, grupos focados em cibercrime podem, eventualmente, atenderem a demandas diretas ou indiretas de autoridades estatais, assim sendo uma mão de obra relativamente barata a um custo político baixo (o suposto não-envolvimento).

Assim sendo, entende-se que os Estados, principais atores do sistema mundo, estão ativamente buscando ampliar sua esfera de influência e capacidade de ação no ciberespaço. Com a tabela de Maness, pudemos observar como se dão as qualidades específicas dos principais atores neste cenário, e entende-se que mesmo não sendo o Estado mais avançado tecnológicamente, a Rússia, pela combinação de fatores, é o ator mais capaz no ciberespaço. No próximo capítulo, observaremos como as autoridades russas tratam públicamente o ciberespaço e as operações cibernéticas, assim como nos adentraremos nas capacidades cibernéticas russas, suas operações internas e externas, e seus efeitos nas relações internacionais contemporâneas.

4 A nova Rússia e as relações cibernéticas internacionais

Em 26 de março de 2000, pouco após a virada do milênio, Vladimir Vladimirovich Putin era eleito presidente da Federação Russa. Um ano antes, ele havia sido apontado como Primeiro Ministro pelo então presidente Boris Yeltsin, e em virtude da renúncia de Yeltsin no mesmo ano, exerceu poderes presidenciais até a eleição de 2000. Vladimir Putin é um ex-agente da KGB, o serviço secreto de segurança da União Soviética, e protagonizou uma rápida ascensão até chegar ao posto máximo da jovem Rússia pós-soviética. Vladimir Putin está no poder há 17 anos, e o que poderia ser um governo instável, se tornou um regime bem estabelecido. No mundo ocidental contemporâneo, Vladimir Putin é figura popular no imaginário da sociedade, sendo constante fonte de notícias que vão desde fotos suas pescando sem camisa até críticas pesadas por políticas internas e receios de um suposto expansionismo russo.[76] De fato, Vladimir Putin é um tipo de celebridade global.[77]

Para entendermos as capacidades cibernéticas da Rússia contemporânea, devemos compreender o processo político interno e a sociedade russa no mundo pós-guerra fria, para assim analisarmos corretamente o comportamento russo na internet e suas interações com o ciberespaço. Putin, por obviedade, está no centro desta discussão, já que comanda a Rússia a quase duas décadas. Efetivamente, Vladimir Putin se tornou um tipo de ícone místico no noticiário de boa parte do mundo, e de fato, modificou a percepção da Rússia tanto internamente, isto podendo ser observado pelos índices de aprovação, quanto externamente, no imaginário de nações pelo mundo afora.

Quando ele assumiu o poder, em 1999, a Rússia passava por grave crise. A guerra na Chechênia, o *default*[78] econômico e os conflitos ideológicos pelas políticas de Yeltsin tornavam o país em um perigoso terreno político. Após o fim da União Soviética, em 1991, Boris Yeltsin, o primeiro presidente eleito, havia implementado uma série de mudanças nas políticas macroeconômicas e na política externa da Federação Russa. Se abrindo aos mercados e ao capitalismo, Yeltsin tentou aplicar medidas liberais em boa parte do aparato estatal russo, que na verdade, era um recém-nascido.[79] Quando Yeltsin tentava aderir a Rússia ao capitalismo

[76] The Economist. The birth of a Tsar. 2017. Disponível em: https://www.economist.com/news/leaders/21730645-world-marks-centenary-october-revolution-russia-once-again-under-rule
[77] CNN. Vladimir's Vacations. 2017. Disponível em: http://edition.cnn.com/2017/08/05/politics/putin-vacation-siberia/index.html
[78] Default. Default é o descumprimento de acordos econômicos e transações financeiras, que vinculam credores e devedores. Calote.
[79] DESAI, Padma. Russian retrospectives on reforms from Yeltsin to Putin. 2005. Disponível em: http://faculty.nps.edu/relooney/00_New_13.pdf

neoliberal ocidental, acabou por criar vários inimigos. As medidas liberalizantes que giravam em torno ao mercado e a privatização de vários setores poderiam até não serem tão ruins por serem uma tentativa de inserir a Rússia no novo mundo pós guerra fria, mas a intensidade das medidas, seu *timing* e sua combinação com um gigantesco índice de corrupção administrativa as tornaram extremamente danosas. De fato, na Rússia pós-soviética de Yeltsin, o capital e o poder estatal se juntaram e se tornaram uma inescrupulosa simbiose.[80] A corrupção e as medidas liberalizantes de Yeltsin vendiam a Rússia e seu poder de fato aos interesses mercadológicos, o que, somado à má administração e elevados índices de corrupção local, regional e nacional, causou uma estrondosa crise econômica, que foi amplificada pela guerra separatista na Chechênia. A popularidade e a própria sanidade do então presidente estavam em baixa, e neste cenário, em 31 de dezembro de 1999, Boris Yeltsin abandonou o cargo.

Vladimir Putin era uma figura relativamente nova na política russa. Somente em meados dos anos 90 é que ele deixou seu serviço na KGB, onde exercia cargo alto como operador na Alemanha, para entrar para a vida política. Parte do grupo de Yeltsin, mas aparentemente diferente da imagem já desgastada, de *old school* de Yeltsin, Putin, de 47 anos e recém chegado na política nacional era uma nova esperança para um povo que já não aguentava mais guerras e crises. Em 30 de dezembro de 1999, um dia antes de assumir os poderes presidenciais cedidos por Boris Yeltsin, Putin publicou um texto em jornais russos, entitulado "Rússia na virada do milênio".[81] No texto, o então primeiro ministro argumentou sobre a necessidade de se enquadrar na realidade global capitalista, enquanto também defendendo um maior papel do Estado para guiar a sociedade russa. Para ele, a crise econômica herdada da União Soviética não poderia ser de outra maneira que não fosse difícil, mas a Rússia acabava de passar por um importante processo transitório. O fim da União Soviética, e o fim do governo de Yeltsin e suas políticas exageradamente liberais marcavam o fim de um longo processo de transição do sistema ideológico soviético para um processo de abertura democrática. Putin afirma que o fato de a Rússia estar em grave crise econômica é o preço a se pagar por herdar a economia soviética, que muito focou seus recursos no setor de matérias primas e na indústria de defesa, assim colocando a Rússia atrás de competidores internacionais nas áreas cientifícas, eletrônicas e de comunicação. Para ele, a democracia e os valores de mercado podem ser aplicados na Rússia, e são a solução, mas somente através de "métodos russos". Em essência, o então futuro

[80] Stratfor. The rise and fall of Russian oligarchs. 2009. Disponível em: https://wikileaks.org/gifiles/attach/144/144365_RussianoligarchPDF.pdf

[81] PUTIN, Vladimir. Russia at the turn of the millennium. 1999. Disponível em: http://pages.uoregon.edu/kimball/Putin.htm

presidente defendia alguns valores liberais enquanto planejava aumentar a força do Estado ao expandir seus poderes e sua eficiência. Na prática, isto pode ser observado pela combinação de tecnocratas liberais no comando da economia e de ex-oficiais da KGB no comando da política. Para que a Rússia se recuperasse economicamente e se mantesse a grande potência que é, e "sempre será", nas palavras de Putin, a sociedade civil e as autoridades deveriam concordar em certas questões sociais para efetivar a unidade nacional russa. Putin defende o pluralismo político, mas enxerga no patriotismo e em "acreditar na grandeza da Rússia" como pilares para uma nova nação.

De fato, em meio à grave crise econômica, à guerra na Chechênia e uma grave ruptura ideológica e social muito recente, parece natural imaginar que a população russa gostaria de um pouco de estabilidade. Vladimir Putin oferecia justamente isto. Em um cenário extremizado por ambos os lados ideológicos (no fim da URSS e nas políticas de Yeltsin), uma alternativa centrista, unificadora, parecia ser muito atrativa. Quase que em contraponto em demonstrar a necessidade de se entrar na economia do mercado, Putin afirma que o Estado deve sempre ser forte, como o garantidor supremo de ordem. Ele diz:

> Statism. It will not happen soon, if it ever happens at all, that Russia will become the second edition of, say, the US or Britain in which liberal values have deep historic traditions. Our state and its institutes and structures have always played an exceptionally important role in the life of the country and its people. For Russians a strong state is not an anomaly which should be got rid of. Quite the contrary, they see it as a source and guarantor of order and the initiator and main driving force of any change (PUTIN, 1999).[82]

Essencialmente, o estadismo citado por Putin está envolvido por um grande fortalecimento do aparato estatal em frente à economia privada. Por exemplo, com as medidas liberalizantes de Yeltsin, muitos magnatas russos se tornaram bilionários e praticamente assumiram o controle da máquina estatal. Para Putin, os bilionários poderiam se manter ativos na economia, mas fora da política. Ainda que ajudado a se eleger pelos colegas de Yeltsin, como o bilionário da TV Boris Berezovsky, Putin não tinha qualquer lealdade para com a classe oligarca russa que havia se formado na década de abertura que passara.[83] Vladimir Putin era um

[82] Nossa tradução: Estadismo. Não acontecerá em breve, se isso acontecer, que a Rússia se tornará a segunda edição, digamos, dos EUA ou da Grã-Bretanha em que os valores liberais têm tradições históricas profundas. Nosso estado e seus institutos e estruturas sempre desempenharam um papel excepcionalmente importante na vida do país e suas pessoas. Para os russos, um estado forte não é uma anomalia que deve ser eliminada. Muito pelo contrário, eles o vêem como uma fonte de garantia da ordem e do iniciador e principal força motriz de qualquer mudança

[83] Foreign Affairs. Putin and the Oligarchs. 2004. Disponível em: https://www.foreignaffairs.com/articles/russia-fsu/2004-11-01/putin-and-oligarchs

oficial da KGB, e a ideia de uma nação poderosa, grandiosa e com status de superpotência era essencialmente forte no imaginário dos envolvidos nos serviços de inteligência da União Soviética. De fato, este sentimento é inerente a muitos dos russos comuns. Assim sendo, Putin entendia a necessidade de abertura da economia, mas não aceitaria se tornar uma marionete dos oligarcas russos que falharam em prever a capacidade do novo presidente. A forma de se controlar esta situação seria fortalecer o Estado e aumentar seu papel nas questões econômicas e sociais. Putin, em sua essência, combinava os melhores aspectos de cada entendimento político para se tornar uma opção muito viável e popular.

Neste contexto de crise econômica, o apelo à unidade e o ataque ao controle do Estado pelo capital, Putin agia para normalizar as coisas na Rússia e consolidar seu poder através do mecanismo estatal. O que o novo presidente gostaria era de uma coesão nacional para que o país pudesse se desenvolver, e sinalizar que este período transitório acabara e delínear os planos para o futuro nacional significava trazer paz e normalização da política na Rússia. Vladimir Putin, através deste processo de normalização e fortalecimento do Estado e da sociedade russa, acabou por realizar o que desejava: a Rússia seria novamente um grande ator internacional. Para que isto se concretizasse, seria necessário fortalecer a atuação do Estado em várias áreas sociais e econômicas, como a regulamentação da mídia e o controle de empresas poderosas em alguns setores, como a distribuição de gás natural. Na visão de Vladimir Putin, Boris Berezovsky jamais poderia ser o dono da televisão na Rússia se a administração quisesse ter algum controle de fato sobre a opinião pública e os rumos da discussão nacional. Em 2003, o Reino Unido garantia asilo político ao então magnata da televisão russa. Berezovski havia fugido da Rússia em meio à acusações de fraude fiscal.[84] De fato, o Kremlin estatizou a rede de televisão de Berezovski, como havia feito com outra rede de televisão e outro magnata pouco antes.[85] As medidas podem ser alvo de críticas, mas as novas autoridades haviam visto de perto como os oligarcas controlavam as políticas no Kremlin, e haviam presenciado o perigo para o funcionamento prático das instituições do Estado que estes homens apresentavam. Ao estatizar a rede de televisão, Putin fazia a única coisa que poderia fazer baseando-se em suas crenças e no seu plano nacional de desenvolvimento. Ainda que sendo uma atitude consideravelmente antidemocrática em essência, a resposta veio à uma ameaça mais antidemocrática ainda, poderia um observador imaginar.

---

[84] The Guardian. Oligarch flees Russia for new life in Britain. 2009. Disponível em: https://www.theguardian.com/world/2009/jan/27/russia-kremlin-oligarchs

[85] ABC News. Government Takes Russia's NTV. Disponível em: http://abcnews.go.com/International/story?id=81235

Assim como com a mídia televisiva controlada inteiramente pelo capital, a questão da privatização de recursos geoestratégicos seria firmemente combatida. A estatal Gazprom, uma empresa de energia, a maior exportadora de gás natural do mundo, foi fortalecida, onde Putin parecia lidar diretamente com as questões administrativas, por vezes. De fato, o Estado russo, para atingir seus objetivos, parecia ter logo percebido que necessitaria controlar os recursos naturais e utilizá-los para tirar o país da crise. Parece ter sido logo na infância de sua presidência que Vladimir Putin havia percebido que a geopolítica energética seria essencial para se atingir o objetivo de uma grande Rússia no cenário internacional e uma economia estável em território nacional, como colocado por Maness. Neste cenário, Vladimir Putin agiu como o normalizador da política na Rússia. Para Sakwa:[86]

> All of the above suggests that politics have now become ‘normal’, in the sense that larger constitutional questions over the shape of the polity have now given way to governmental administration of more mundane policy questions and the management of a functioning market economy based on private property and international economic integration (SAKWA, 2004, p.58).[87]

É possível observar que os recém-chegados ao poder queriam se afastar o mais cedo possível do enorme período de turbulências que assolou o país durante toda a década de 90. Na virada do milênio, Vladimir Putin não poderia ter momento melhor para delinear sua visão de país, estabelecer as diretrizes da nova Rússia pós-soviética, enquanto que mantinha a base constitucional da época de Yeltsin e aumentava sua popularidade como um líder duro, porém justo. Ao estatizar setores que ficaram famosos por enriquecer poucos homens em detrimento da maioria dos russos e seus interesses, Putin conseguiu estabilizar o país, impulsionado por melhorias econômicas em seus primeiros anos de governo. Além disso, "economia das sombras" (Sakwa 2004, p.50), oriunda de atividades do crime organizado, movia cerca de 40% da economia na Rússia no momento em que Putin assumiu o governo. Este cenário era propício para que o ex-agente secreto pudesse fortalecer as agências de segurança e o combate ao crime. De fato, Putin não escondia a sua forte política de segurança interna, e a FSB, a sigla para o serviço federal de segurança russo, que substituiu a extinta KGB, foi se tornando cada vez mais

[86] SAKWA, Richard. Putin: Russia’s Choice. Routledge, London. 2004.
[87] Nossa tradução: Tudo o que precede sugere que a política tornou-se agora "normal", no sentido de que as maiores questões constitucionais sobre a forma da política já deram lugar à administração governamental de questões políticas mais mundanas e à gestão de uma economia de mercado funcional baseada em propriedades privadas e integração econômica internacional.

protagonista em situações que vão desde o desmantelamento de gangues criminosas, monitoramento de suspeitos até a apreensão de bens de oligarcas exilados.[88]

Essencialmente, as mudanças na Rússia ao virar do milênio passavam muito pelo fortalecimento do poder executivo. Primeiramente, é necessário considerarmos a história do território, onde mesmo não entrando em maiores detalhes neste trabalho, se apresenta como uma necessidade observar que desde o imperialismo dos tsars, passando pelo autoritarismo comunista e chegando até a oligarquia do capital corrupto, gerações de milhões de russos viveram sob comando firme. A mão de ferro de Stalin pode ser hoje fonte de séries e mais séries de textos e documentários sobre a violência autoritária de um regime no mínimo contraditório, mas parece ser cotidiano para os russos vivendo na Rússia, se observarmos sua história. Desde os tempos de corrupção soviética, até o momento de unificação do capital de mercado com o poder estatal da década de 90, interessados em mudar o cenário para melhor na Rússia enfrentaram com grande dificuldade o fantasma da corrupção institucionalizada. Há de se entender, também, que no aparato administrativo deixado por Yeltsin as mudanças eram controladas por grupos conectados perigosamente ao capital estrangeiro, e um fator balanceador teria de ser imposto. Além disto, a incidência da atuação do crime organizado e sua relação com autoridades, além de em suma, movimentar boa parte da vida em sociedade para uma camada da população, apresentava-se como um forte desafio para garantir a própria existência do Estado. Quando Vladimir Putin chegou ao poder, viu no fortalecimento do poder executivo como seu principal aliado em estabilizar e guiar a Rússia. Ele disse, em 1999:

> Another serious problem is inherent in that tier of authority which the government belongs to. The global experience prompts the conclusion that the main threat to human rights and freedoms, to democracy as such emanates from the executive authority. Of course, a legislature which makes bad laws also does its bit. But the main threat emanates from the executive authority. It organizes the country's life, applies laws and can objectively distort, substantively and not always maliciously, these laws by making executive orders.
> The global trend is that of a stronger executive authority. Not surprisingly, society endeavors to better control it in order to preclude arbitrariness and misuses of office. This is why I, personally, am paying priority attention to building partner relations between the executive authority and civil society, to developing the institutes and structures of the latter, and to waging an active and tough onslaught on corruption (PUTIN, 1999).[89]

[88] The Guardian. FSB: Vladimir Putin's immensely powerful modern-day KGB. 2013. Disponível em: https://www.theguardian.com/world/2013/oct/06/fsb-putins-modern-day-kgb

[89] Nossa tradução: Outro problema sério é inerente ao nível de autoridade a que o governo pertence. A experiência global leva à conclusão de que a principal ameaça para os direitos humanos e as liberdades, para a democracia como tal, emana da autoridade executiva. Claro, uma legislatura que faz leis ruins também faz pouco. Mas a principal ameaça emana da autoridade executiva. Ele organiza a vida do país, aplica leis e pode distorcer objetivamente, substancialmente e nem sempre maliciosamente, essas leis fazendo ordens executivas.A tendência global é a de uma autoridade executiva mais forte. Não surpreendentemente, a sociedade se esforça para controlá-

De fato, o poder executivo de Putin se mostra como natural e necessário para que o Kremlin possa exercer sua autoridade. Quando, pouco após assumir o poder, a administração estatiza gigantes da mídia, óleo e gás natural, a própria força do poder executivo vem à tona. Para mudar a Rússia, de fato, seria uma necessidade tomar medidas difíceis. Quando necessitava de maior lealdade na gigante Gazprom, Putin nomeou seu amigo de longa-data, Alexey Miller, para o posto de conselheiro-chefe. Foi apenas uma de muitas mudanças realizadas pelo poder executivo na administração das grandes empresas na Rússia. Para que sua visão pudesse ser aplicada, precisava tomar medidas autoritárias, mas que devido ao histórico do país e às formas como cresceram algumas destas empresas, as medidas seriam vistas como populares, e o presidente ia ganhando mais força.

Sendo um ex-coronel da KGB, e tendo chefiado a FSB anos atrás, Putin se cercou com oficias de inteligência.[90] A FSB, o serviço de segurança federal, ganhou mais poder e passou a atuar de diversas maneiras, desde proteger o território de espiões, desmantelar grupos considerados perigosos, até monitorar alvos identificados e operacionalizar ações invasivas. Enquanto que os estereótipos são perigosos, é necessário entendermos que a mente dos agentes de segurança envolve, em boa parte, uma boa dose de patriotismo e outra boa dose de controle.[91] Neste cenário, em que a Rússia elegeu Putin a salvá-la, as forças de segurança teriam um papel essencial para que a administração, seus planos, e até mesmo a coesão nacional permanecessem vivas em um cenário onde vários atores perigosos poderiam agir, como bilionários revoltosos ou Estados inimigos. A instabilidade na Rússia, derivada das décadas de retrocesso, só poderia ser combatida com um forte poder executivo garantido pela lealdade das forças de segurança. Não foi diferente. Vladimir Putin, o agente secreto, se tornou presidente da Rússia e um dos homens mais poderosos do mundo. A Rússia, lentamente, se recupera. A FSB, de fato, desde as operações internas para conter opositores, até supostas operações externas para assassinar traidores, se tornou um braço do poder executivo na Rússia , e pelo contexto histórico, poucas medidas como as tomadas pelo Kremlin nos últimos anos poderiam ser tão efetivas. É importante que entendamos o papel da FSB e do entendimento de governo da administração de

---

la melhor, a fim de impedir a arbitrariedade e os abusos do cargo. É por isso que, pessoalmente, estou prestando atenção prioritária à construção de relações de parceiros entre a autoridade executiva e a sociedade civil, para o desenvolvimento dos institutos e estruturas deste último, e para fazer um ataque ativo e duradouro à corrupção.

[90] DAWISHA, Karen. Putin's Kleptocracy. New York. 2016.

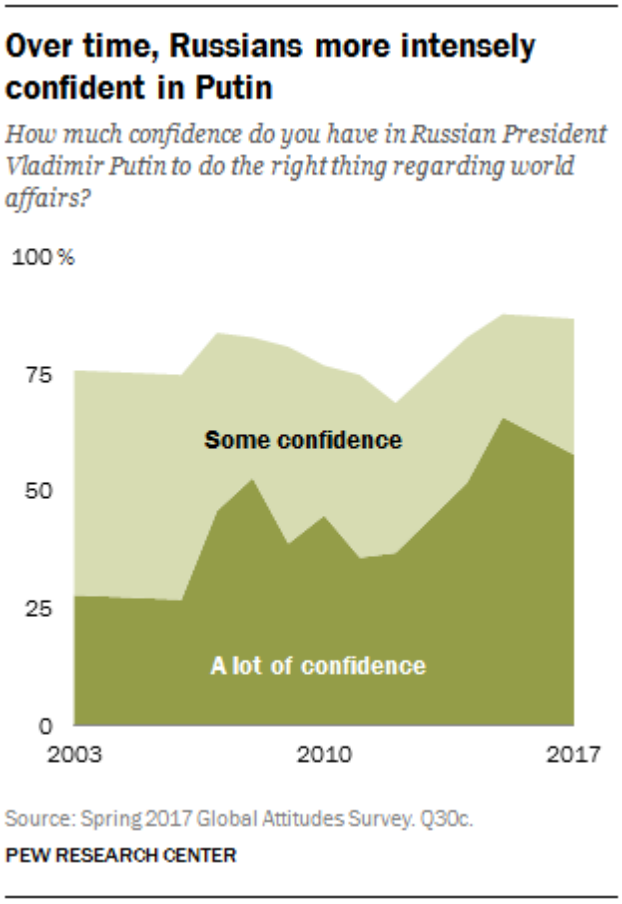
[91] NEWTON, Matthew. Russia Media Profile: Digital patriotism and Nationalist Agenda. 2017. Disponível em: https://jsis.washington.edu/news/russia-media-profile-digital-patriotism-nationalist-agenda/

Putin pois estes tem papel direto nas relações cibernéticas internacionais, e no ciberespaço como um todo, como veremos mais a frente.

Em 12 de maio de 2000, 5 dias após a formalização da presidência de Vladimir Putin, agentes federais de segurança, armados, invadiram a sede do maior império privado de mídia na Rússia, a NTV. Na época, o oficial de comunicações da FSB, Aleksandr Zdanovich, afirmou que foram encontrados documentos com evidências de corrupção de grandes nomes da empresa.[92] Seria o fim do império midiático de Vladimir Gusinsky, então bilionário que havia feito fortuna na década passada. Gusinsky acabou preso e libertado várias vezes, e sua influência política parecia ter acabado. A ação realizada pelos agentes de segurança, uma das primeiras da nova administração federal, mostra como seriam tratados até mesmo os mais ricos que se opusessem ao Kremlin. Justificativas e reações internacionais à parte, o novo modo de agir das autoridades agradava a maioria da população. Temos de considerar, como colocado anteriormente, o contexto histórico. O país em que Putin e seus colegas cresceram não lhes ensinou outro modo de fazer política, e a necessidade de controlar boa parte da sociedade seria uma das principais características do novo governo. Quando afirma que o poder executivo ganhará força, e ampliará o diálogo com a sociedade civil em uma conexão direta, Putin não escondeu que as autoridades executivas agora desempenhariam um papel mais atuante na Rússia. Há de se entender também, que os números o apoiam:

[92] NY Times. Russian security agencies raid media empire's offices. 2000. Disponível em: http://www.nytimes.com/2000/05/12/world/russian-security-agencies-raid-media-empire-s-offices.html

Figura 8 – Confiança dos russos em Putin



Fonte: Pew Research Center. 2017. s/p.

Segundo a pesquisa da Global Attitudes e do PEW Research Center, mais de 75% dos russos tem algum tipo de confiança em Vladimir Putin. O número dos que confiam muito no presidente foi aumentando gradualmente ao passar dos anos. Podemos entender que boa parte do sistema de sociedade na Rússia, por um bom tempo, apresentou características autoritárias por parte das autoridades, e quando Putin coloca, antes de iniciar seu governo, que agora o país entraria em um caminho à democracia, porém de maneira russa, dá a entender que a sociedade entenderia e apoiaria medidas contraditórias aos olhos de ocidentais. É claro que este tipo de comportamento abre precedentes perigosos, mas ignorar o contexto em que a administração se encontrou seria tornar este trabalho em algum tipo de propaganda ocidental que não observa todos os fatos.

Para alguns autores, esta interessante união entre o poder executivo e as forças de segurança federais prejudicam a tentativa de democratizar a Rússia. O controle inibe a

liberdade. Sendo nomeada de ditadura pós-moderna[93], democracia gerenciada[94], democracia eleitoral[95] e até mesmo uma cleptocracia[96], a administração de Vladimir Putin realmente exerce um demasiado controle sobre boa parte da sociedade. A liberdade de expressão é relativa, e opositores podem acabar sendo presos ou até mesmo mortos. O ex agente da FSB, Alexander Livtnenko, fugiu para Londres em exílio. Em 23 de novembro de 2006, foi envenenado e morreu no Reino Unido.[97] Em 2015, o político opositor Boris Nemtsov foi assassinado, perto do Kremlin, na noite de 27 de fevereiro.[98] Ainda que estes fatos não possam ser conectados oficialmente ao Kremlin, o clima de liberdade de expressão não parece ser dos melhores na Rússia.

De fato, o controle exercido pelas autoridades em diversas áreas da sociedade torna impossível não realizar uma conexão entre o passado do presidente e seu grupo de confiança para com a realidade administrativa do país. Somente o que está sob controle é que parece seguro, na instável Rússia pós-crise. Enquanto que o desejo ou não de implementar uma democracia *de facto* em seu país seja uma incógnita, Vladimir Putin fez o que precisava fazer para estabelecer seu regime e manter suas diretrizes como o foco do país. Neste processo transitório, pode-se entender que a Rússia realmente apresenta características de uma "democracia gerenciada", mas na visão deste trabalho, realizando uma contextualização histórica, não poderia ser diferente.

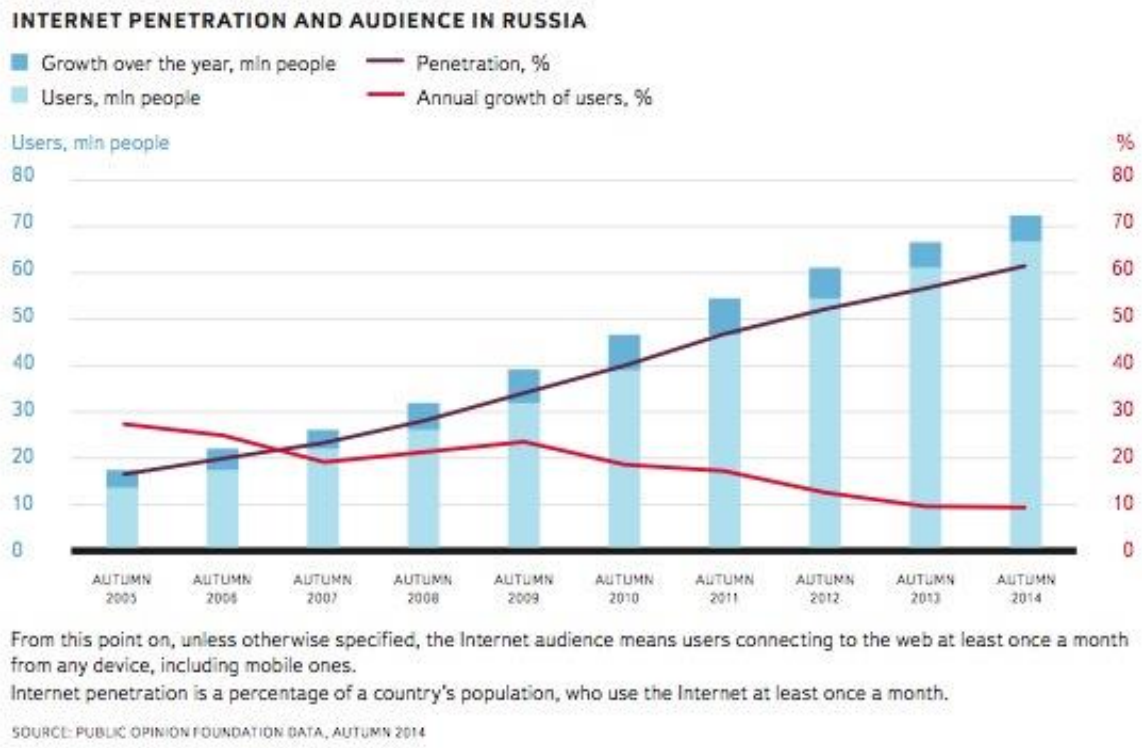
4.1 Internet em alta

Neste contexto transitório, saindo de um período de várias incertezas, é que a Rússia presencia e também faz parte do fenômeno global que foi o surgimento e desenvolvimento da internet. Nos anos 2000, o mundo todo viu o boom tecnológico da internet atingir os quatro cantos do planeta, ampliando o acesso à rede e a tornando quase que um fator natural nas sociedades humanas contemporâneas. Na Rússia de Putin, assim foi a evolução:

---

[93] POMERANTSEV, Peter. Russia: A post-modern dictatorship? 2013.
[94] LIPMAN, Masha. “Managed Democracy” in Russia. 2001.
[95] LUKIN, Alexander. Electoral Democracy or Electoral Clanism? Disponível em: http://www2.gwu.edu/~ieresgwu/assets/docs/demokratizatsiya%20archive/07-01_lukin.pdf
[96] DAWISHA, Karen. Putin’s Kleptocracy. 2014.
[97] BBC. Alexander Livtinenko: Profile of murdered russian spy. 2016. Disponível em: http://www.bbc.com/news/uk-19647226
[98] The Guardian. Nemtsov family dismisses verdict. 2017. Disponível em: https://www.theguardian.com/world/2017/jun/29/gunman-found-guilty-murdering-russian-opposition-leader-boris-nemtsov

Figura 9 – Internet na Rússia



Fonte: Public Opinion Foundation. 2014. s/p.

Segundo o gráfico, 10% da população russa tinha acesso à internet em 2005. Em 2014, o número chegou a 75%. De fato, a internet era uma realidade na nova Rússia, também. Aqui é que se faz necessário entendermos os tempos conturbados citados anteriormente, pois com o desenvolvimento da internet, como já abordado neste trabalho, abre-se espaço para um fluxo de informações muito maior e mais intenso. Quando a mídia convencional foi estatizada anteriormente, um dos objetivos era justamente abafar opositores indesejados, e a internet abria espaço exatamente para isto. Pela natureza da plataforma, e com o descrédito da mídia televisiva em ascenção, as mídias sociais da internet se tornaram essenciais para a discussão política, isto no mundo todo, incluindo-se na Rússia. Como muito acontece em outros países, como por exemplo nas revoltas que levaram à Primavera Àrabe, grupos se organizavam e até mesmo se financiavam através de plataformas online, como o Facebook. Na Rússia, isto logo se tornou um problema.

Após as eleições parlamentares russas de 2011, grandiosos protestos, segundo autores, os maiores desde a queda da União Soviética, atingiram o país.[99] Boa parte deles foi organizado

[99] BBC. Russian election: biggest protests since fall of USSR. 2011. Disponível em: http://www.bbc.com/news/world-europe-16122524

por redes sociais da internet, e após estes eventos, o Kremlin passou a regular o acesso à certas informações na internet com muito mais frequência. Em 2014, Emily Parker escreveu sobre a "*Cyberphobia*" de Vladimir Putin, onde a autora indica que a administração passou a temer pela estabilidade do regime ser posta em perigo pelas ações de grupos online e em reação, começou a controlar imensamente o acesso à internet.[100] De fato, as autoridades russas criaram uma série de leis para regulamentar o acesso online, e inibir o acesso a alguns conteúdos, como por exemplo, a atual guerra na Ucrânia.

Uma destas mídias sociais é o website Vkontakt, ou o VK, que funciona como o Facebook, na versão russa. Na Rússia é a rede social mais utilizada, e ultrapassou 400 milhões de contas ativas em 2017.[101] Em 2014, quando seu idealizador e fundador, Pavel Durov, se recusou a entregar informações sobre possíveis terroristas ucranianos, a administração agiu. Durov foi obrigado a vender a empresa para o grupo Mail.ru, que tem conexões com o Kremlin, e deixou o país em "exílio auto-imposto", para nunca mais voltar, já que, segundo o próprio, "infelizmente, o país é incompatível com negócios na internet atualmente".[102] As autoridades não hesitaram em tomar uma ação contra a maior empresa de redes sociais do país para garantir o mero acesso à algumas informações necessárias. De fato, a internet, ao que parecia, seria mais um setor estatizado na Rússia de Putin. É claro, no entanto, que como já observamos, as coisas não são tão simples no mundo cibernético.

Na visão aqui apresentada, a "*ciberphobia*" de Putin apresentada por Parker está equivocada. Enquanto que é verdade que o Kremlin teme pela sua estabilidade e sua relação com as atividades online, imaginar que as autoridades tratam do assunto apenas de maneira reativa parece ingênuo. A fobia, se existente, se traduziu em uma intensificação da presença de agentes do governo na internet e um delineamento de estratégias defensivas e ofensivas para agir no ciberespaço. Nos protestos de 2011, citados anteriormente, é possível identificar que websites de jornais liberais e uma TV pela internet de cunho opositor à administração foram "alvos de ataques DDoS sofisticados" (Shakarov, 2013, p.53). De fato, após Dimitri Medvedev ser eleito presidente em 2008, a relação do Kremlin com as operações no ciberespaço só se intensificaria, visto o foco do novo presidente em desenvolver a tecnologia cibernética da Rússia.[103] Em essência, o Kremlin havia percebido que necessitaria se adentrar mais ainda neste

[100] PARKER, Emily. Putin's Cyberphobia. 2014.
[101] VK. User catalog. 2017. Disponível em: https://vk.com/catalog.php
[102] TechCrunch. Durov out of VK for good. 2014. Disponível em: https://techcrunch.com/2014/04/22/durov-out-for-good-from-vk-com-plans-a-mobile-social-network-outside-russia/
[103] CNN. Medvedev wants Russia to go hi-tech. 2009. Disponível em: http://edition.cnn.com/2009/WORLD/europe/11/12/russia.medvedev.speech/

mundo para não correr riscos e ainda obter algumas vantagens. Medvedev chegou a afirmar que "o computador agora é mais importante do que rifles." (REVERON, 2013, p.7).

Neste cenário é que o alto índice de controle sobre a sociedade que a administração exerce entra em jogo. A aplicação de novas leis, regulamentações, e o controle de informações como um todo criam um ambiente favorável para também agir dentro da internet. Com o tempo, boa parte do tráfego online na Rússia passou a ser monitorado pela FSB (Maness, 2013), e o leque de ações se abriu. Aqui é onde entra a interessante simbiose citada por Nye (2009, p.12) e apresentada no capítulo anterior, onde o governo russo utiliza de recursos não-estatais, principalmente recursos humanos e hardware, para atingir objetivos favoráveis ao regime. Por exemplo, por mais de uma vez foi identificada a ação de indivíduos onde estes, de maneira incessante, provocam discussão política com um determinado objetivo. Estes, chamados trolls, praticam o ato de polarizar uma discussão ou dar a impressão de um maior apoio à determinada opinião, então prejudicando o processo de discussão política real. Na Letônia, houveram acusações governamentais de que trolls russos estariam agindo incessantemente na internet e prejudicando o processo democrático, muito como parece ter ocorrido no caso dos bots das eleições francesas citadas aqui anteriormente.[104] De fato, os *trolls* e os *bots* cumprem quase que a mesma função, apesar de que no caso dos trolls, a aparência de realidade e a capacidade de fomentar uma discussão maior ainda é mais elevada, mas entraremos nesta discussão no próximo subcapítulo.

Em síntese, percebe-se na Rússia uma convergência de interesses entre os atores não estatais e estatais, por vezes. Como dito por Nye, muitas vezes o governo russo ignora ou protege atores criminosos no ciberespaço, e na verdade acaba por passar a contar com seus serviços. É assim que se o Kremlin acaba por criar um ciber-exército. Por exemplo, o grupo Fancy Bear, acusado pela mídia e governo dos EUA de estar por trás de boa parte dos vazamentos da NSA que afetaram as eleições de 2016, é famoso na Rússia, e não tem qualquer conexão oficial com o Kremlin, já exercendo atividades anteriores e por vezes de cunho apolítico.[105] Entende-se, é claro, que a probabilidade de que o governo tenha seus agentes de confiança próprios é alta, mas compreender a cooperação entre os diferentes atores é essencial para entedermos a força da Rússia no ciberespaço. Estes atores acabam por criar uma grandiosa capacidade ofensiva, como colocado por Maness. Impulsionados pelo patriotismo e por vezes pelo isolacionismo do resto do mundo, hackers russos podem agir por si só e acabar por serem

[104] FOKIN, Alexander. Internet Trolling as a tool of hybrid warfare: The case of Latvia. NATO Strategic Communication Centre of Excellence. 2016.
[105] Wired. Russia's Fancy Bear hackers. Disponível em: https://www.wired.com/story/fancy-bear-hotel-hack/

benéficos ao regime de Vladimir Putin, como aconteceu na Estônia, em 2007, caso que estudaremos pouco mais à frente.

Essencialmente, compreendemos como a ascenção de Vladimir Putin ao poder se deu, e qual é a sua visão para a Rússia. O histórico do país e a nova administração mostram que o Kremlin tem muito espaço para manobrar confortavelmente em decisões políticas, que podem afetar os russos e também o resto do mundo. Vivenciando o fenômeno global do ciberespaço, o Kremlin aprendeu, sob necessidade, que uma maior inserção no ciberespaço seria também uma oportunidade. Ao se tornar pioneiro em utilizar táticas específicas de coerção política ou até mesmo de intimidação ideológica, o governo aprendeu como operar no ciberespaço rapidamente. Por vezes, internamente, como nos protestos de 2011, e por vezes, externamente como na Letônia. De fato, pelo interessante desenvolvimento do ciberespaço russo e sua conexão com as forças de segurança e o poder executivo, as capacidades cibernéticas da nova Rússia se tornaram amedrontadoras do ponto de vista inimigo. No subcapítulo seguinte, observaremos como de fato a Rússia se envolve no ciberespaço, seu pensamento sobre este, suas armas e como as utiliza para atingir objetivos internos e externos.

4.2 Ciberespaço russo: conceitos, estratégias e efeitos

Observamos o nascimento e o crescimento da internet, e em que contexto isto se deu, na Rússia. Pudemos entender como o Kremlin aprendeu que as operações no ciberespaço estão muito conectadas às operações de informação, sendo uma parte destas. Entendendo o papel cada vez mais intensificado e importante do ciberespaço no sistema mundo, a doutrina militar da Federação Russa de 2010, aprovada pelo então presidente Dimitri Medvedev, diz:[106]

> [Priorities of the armed forces] d) the prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favourable response from the world community to the utilization of military force (RUSSIAN MILITARY DOCTRINE, 2010).[107]

Ao analisarmos, a relação é clara: O entendimento dos militares russos sobre as operações de cyberwarfare estão muito conectadas às operações informacionais. Muito como

[106] Doutrina militar russa. 2010. Moscou. Disponível em: http://carnegieendowment.org/files/2010russia_military_doctrine.pdf

[107] Nossa tradução: [Prioridades das forças armadas] d) A implementação prévia de medidas de guerra de informação para alcançar objetivos políticos sem a utilização da força militar e, posteriormente, no interesse de moldar uma resposta favorável da comunidade mundial à utilização de força militar (DOUTRINA MILITAR RUSSA, 2010).

observamos nos protestos anti-Putin de 2011, a Rússia havia percebido anteriormente que operacionalizar atividades no sentido de controlar, modificar ou expor informações era uma arma tão importante como qualquer outra. Objetivos políticos poderiam ser atingidos, em casa, e lá fora. "Moldar" uma resposta favorável do mundo às ações militares russas. As autoridades não poderiam ser mais claras: As operações de informação servem também para atingir objetivos políticos internamente e externamente. Ao contrário do entendimento de ciberespaço para os Estados Unidos, no qual não entraremos em grandes detalhes, mas cabe dizer que há uma clara separação entre as operações de informação e operações cibernéticas (em geral, as operações cibernéticas são demasiadamente secretas também), a proposta russa para atuação no ciberespaço é ampla. Para exemplificar, citamos David Smith:[108]

> The second basic point is that Russia holds a broad concept of information warfare, which includes intelligence, counterintelligence, deceit, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, degradation of information systems and propaganda. Computers are among the many tools of Russian information warfare, which is carried out 24 hours a day, seven days a week, in war and in peace. Seen this way, distributed denial of service (DDoS) attacks, advanced exploitation techniques and Russia Today television are all related tools of information warfare (SMITH, 2012, p. 9).[109]

Quando Dimitri Medvedev afirmou que computadores eram tão importantes quanto rifles, não parecia ser brincadeira. O Kremlin passou a tratar as operações cibernéticas como uma importante arma de seu arsenal em guerras internas e externas. Ainda, há de se entender que estas operações são aplicadas previamente a cenários de guerra, na realidade, como posto por Connell:[110]

> By implication, the tools of information warfare can—in fact, should—be brought to bear before the onset of military operations in order to achieve the state's objectives without having to resort to the use of force, or, should force be required, disorienting and demoralizing the adversary and ensuring that the state is able to justify its actions in the eyes of the public. Thus, information warfare, and by extension cyber, becomes

---

[108] SMITH, David. How Russia Harnesses Cyberwarfare. 2012. Disponível em: http://www.afpc.org/files/august2012.pdf

[109] Nossa tradução: O segundo ponto básico é que a Rússia possui um amplo conceito de guerra de informação, que inclui inteligência, contra-inteligência, engano, desinformação, guerra eletrônica, debilitação de comunicações, degradação de suporte de navegação, pressão psicológica, degradação de sistemas de informação e propaganda. Os computadores estão entre as muitas ferramentas da guerra de informação russa, que é realizada 24 horas por dia, sete dias por semana, em guerra e em paz. Visto desta forma, os ataques distribuídos de negação de serviço (DDoS), as técnicas avançadas de exploração e a televisão Russia Today são todas ferramentas relacionadas à guerra informacional.

[110] CONNEL, M; VOGLER, S. Russia's approach to cyberwarfare. 2017. Disponível em: https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf

> a legitimate tool of the state in peacetime as well as wartime (CONNELL, 2016, p. 12).[111]

De fato, o que isto nos mostra é que as operações cibernéticas russas teriam um escopo de ação ininterrupto, não sendo limitadas à operações com alvos bem definidos, apesar de estas ocorrerem, por obviedade. Aqui, entender os procedimentos que entendemos no capítulo anterior se faz necessário. Boa parte das capacidades ofensivas russas passa pela forma que se deu a formação da sociedade contemporânea e pela ação de grupos específicos dentro do ciberespaço em seus anos de infância, que foram os mesmos do regime de Vladimir Putin. Grupos autônomos de hackers, que podem conduzir APTs, existem em grande número, e cibercriminosos obtém um ótimo tratamento por parte das autoridades, se os interesses se convergirem (Nye, 2009). Smith diz:

> Russia is a typical extractive economy that still enjoys the benefits of the quite good Soviet educational system. Great wealth is concentrated in the hands of a few, while many people with training in math, science and computers look for work. The result is a thriving botnet-for-hire industry (SMITH, 2017, p. 10).[112]

Essencialmente, hackers mercenários existem em todos os lugares do mundo, mas na Rússia parecem ter atenção especial. Quando famosos grupos como o *Fancy Bear* realizam algum tipo de operação, não se pode verdadeiramente conectar este grupo ao Kremlin, não de maneira totalmente satisfatória, ao menos. Esta característica, em convergência com o fato de que hackers, ou simplesmente usuários da internet, possam ser contratados à um baixo custo e operacionalizem alguma ação benéfica ao governo, como aconteceu com os *trolls* da Letônia observados anteriormente, acaba por criar um grande e interessante campo de ações para um ator como Moscou. Ao "delegar" parte de suas operações à terceiros, fica livre da culpabilidade, que já é difícil de ser demonstrada no ciberespaço por natureza, além de atingir determinado objetivo a um baixo custo financeiro, e político. Ainda, o fator patriótico que observamos neste capítulo é outro que pode entrar em jogo, quase que recrutando *cyber-tropas* naturalmente para o Kremlin. Quando o assunto é algo que afeta o emocional de russos, atores individuais ou grupos nacionalistas de hackers podem tomar ação por si só seja utilizando *botnets*, organizando

[111] Nossa tradução: Por implicação, as ferramentas da guerra da informação podem - e de fato, devem ser levadas antes do início das operações militares, a fim de alcançar os objetivos do estado sem ter que recorrer ao uso da força, ou, se for necessário, desorientar e desmoralizar o adversário e garantir que o Estado seja capaz de justificar suas ações aos olhos do público. Assim, a guerra da informação e, por extensão, a guerra cibernética, torna-se uma ferramenta legítima do estado em tempo de paz, bem como em tempos de guerra

[112] Nossa tradução: A Rússia é uma economia extrativa típica que ainda goza dos benefícios do sistema educacional soviético bastante bom. Grande riqueza está concentrada nas mãos de alguns, enquanto muitas pessoas com treinamento em matemática, ciência e computadores procuram trabalho. O resultado é uma próspera indústria de botnets-para-contratar.

ataques DDoS ou realizando uma campanha de desinformação. Neste cenário, o Kremlin ganha um forte aliado em uma interessante convergência de interesses. Quase que ironicamente, o presidente Vladimir Putin afirmou, em 2017, que hackers patrióticos russos podem ter se envolvido nas eleições dos EUA de 2016.[113] O presidente chegou a dizer que estes hackers, que não teriam envolvimento com o Kremlin, se sentiram ofendidos por determinados atores que se opunham à Rússia e viram em suas ações uma maneira de se manifestar e ajudar o país. "A um nível estatal, não fazemos isto", concluiu.

Mas fazem. De fato, boa parte das campanhas cibernéticas russas envolve atores privados, como o *Fancy Bear* ou o grupo de *trolls*, mas boa parte destas operações tem objetivo de beneficiar o Kremlin de alguma maneira. Essencialmente, a própria doutrina militar afirma que os russos passariam a utilizar *cyberwarfare* para moldar a opinião pública, e facilitar outras operações, como o uso da força. Muito como ocorreu em 2011, o Kremlin passou a tratar da informação e do ciberespaço como um amplo campo para realizar operações e obter certas vantagens, sejam elas políticas ou econômicas. Como observamos no caso dos bots das eleições francesas, as ações dentro do ciberespaço proporcionadas pelo RT e Sputnik estavam bem delineadas para alterar a percepção da opinião pública e desviar o debate para favorecer Le Pen. Tudo isto, é claro, de maneira sutil e com pouca culpabilidade por parte dos envolvidos.

Todas estas características específicas tornam a Rússia como um perigoso ator cibernético. Apesar de contar com os recursos "terceirizados" exemplificados acima, a habilidade governamental de agir no ciberespaço por conta própria não deve ser ignorada:

> The cyber facilities of the communications agency were highly regarded by American experts: It was said to have both the authority and the capability to penetrate all government and private information services in Russia. It also has reportedly been successful in collecting intelligence on foreign business ventures, including confidential bank transactions. Starting in the mid-1990s the communications agency took an interest in controlling the Internet, at least inside Russia. In hearings in 1996, its deputy director, Colonel General Vladimir Markomenko, told the State Duma that "the Internet poses a threat to National Security," and the agency was empowered to monitor electronic, financial, and securities transactions and other communications, including private Internet access. Within this sophisticated agency, the primary concern was not Chechen propaganda but protecting the communications networks from intrusion by foreign intelligence services. The professionals in information security were not interested in being at the vanguard of Russia's cyberwarfare against the Chechens (SOLDATOV, 2011, p. 187).[114]

[113] The Independent. Vladimir Putin hints at 'patriotic' private hackers interference in US election. 2017. Disponível em: http://www.independent.co.uk/news/world/americas/us-politics/vladimir-putin-russian-hackers-patriotic-private-us-election-2016-donald-trump-win-dnc-hillary-a7767436.html

[114] Nossa tradução: As instalações cibernéticas da agência de comunicação eram muito bem avaliadas por especialistas americanos: era dito que tinha autoridade e capacidade para penetrar em todos os serviços públicos e privados de informação na Rússia. Também teria sido bem sucedido na coleta de informações sobre negócios comerciais estrangeiros, incluindo transações bancárias confidenciais. A partir de meados da década de 1990, a

Soldatov nos apresenta um panorama de uma agência de segurança que foi absorvida pela FSB no ínicio do governo de Putin. Os serviços de segurança, mesmo estando em posse de grande capacidade técnica, por vezes parecem preferir não agir em alguns cenários. Seja isto uma estratégia para economizar recursos ou simplesmente pelo fato de que outra tática passou a ser usada, os serviços de segurança, como a FSB, tinham muitos recursos e capacidade de agir. No entanto, preferiram deixar os hackers nacionalistas fazerem o serviço. Sobre a guerra na Chechênia:

> Soon independent hackers, encouraged by the Kremlin, expanded their attacks far beyond Chechen Web sites; the same hackers' groups began to target the Web sites of opposition media and political groups. They targeted extremist groups like the National Bolshevik Party, opposition groups like that of Garry Kasparov, and mainstream media outlets like the newspaper Kommersant and Echo Moskvy radio (SOLDATOV, 2011, p. 187).[115]

Como observado por Soldatov, hackers "independentes" é que agiram neste cenário de polarização contra os rebeldes chechenos. Os serviços de segurança parecem ter ficado apenas no apoio. De qualquer maneira, a lição que surge é a de que o Kremlin, desde o início dos anos 2000, ativamente se envolveu no desenvolvimento de comunidades semi-autônomas de hackers ou usuários independentes para atingir determinados objetivos, como desestabilizar os rebeldes chechenos ou afetar a opinião pública na Letônia. Com o passar do tempo, a tendência de estatizar setores importantes acabou também afetando a internet na Rússia, e o Kremlin se move para não perder as rédeas da plataforma, assim como usá-la como uma importante ferramenta para atingir seus objetivos, sejam eles de política interna ou política externa. A natureza do ciberespaço dificulta gravemente qualquer tipo de atribuição de certas atividades, como ataques DDoS, ao seu autor real. Moscou parece ter entendido este fato rápidamente, e ao longo dos anos, passou a desenvolver técnicas específicas para agir nesta plataforma e além. A própria

agência de comunicação se interessou por controlar a Internet, pelo menos dentro da Rússia. Em audiências em 1996, seu vice-diretor, o Coronel General Vladimir Markomenko, disse à Duma do Estado que "a Internet representa uma ameaça à Segurança Nacional", e a agência estava habilitada a monitorar transações eletrônicas, financeiras e de valores mobiliários e outras comunicações, inclusive privadas no acesso à internet. Dentro desta agência sofisticada, a principal preocupação não era a propaganda chechena, mas proteger as redes de comunicação contra a intrusão por parte de serviços de inteligência estrangeiros. Os profissionais da segurança da informação não estavam interessados em estar na vanguarda da guerra cibernética da Rússia contra os chechenos

[115] Nossa tradução: Em breve, hackers independentes, encorajados pelo Kremlin, ampliaram seus ataques muito além dos sites da Chechênia; os mesmos grupos de hackers começaram a segmentar os sites da mídia da oposição e dos grupos políticos. Eles atacaram grupos extremistas como o Partido Bolchevique Nacional, grupos de oposição como o de Garry Kasparov e os principais meios de comunicação como o jornal Kommersant e o rádio Echo Moskvy

doutrina militar e de segurança de informação na Rússia dão a entender que as autoridades federais passariam a tratar o ciberespaço como uma grande nova zona de influência e ação, e é justamente isso que Vladimir Putin e Dimitri Medvedev fizeram. No próximo subcapítulo, observaremos algumas das ações cibernéticas realizadas no exterior, partindo da Rússia, e como isto afetou os envolvidos.

4.3 De Moscou, com amor

Para Ryan Maness, "o conflito cibernético é a ferramenta de menor custo para a política externa russa".[116] Em abril de 2007, o governo da Estônia decidiu remover um memorial em Talinn, a capital, em homenagem aos soldados soviéticos que liberaram o território dos nazistas na Segunda Guerra. Pouco depois, protestos da minoria étnica de russos que habita no Estado que conseguira a independência da União Soviética em 1991 colocaram o país em uma crise política. Os russos étnicos, que são cerca de 25% da população na Estônia, não reclamavam somente pelo memorial, mas também por uma suposta discriminalização e marginalização por parte do resto da sociedade da Estônia, desde que o país ganhou independência. Logo, os protestos se tornaram violentos e prisões foram realizadas. O Kremlin chegou a protestar sobre a situação, afirmando que o governo reprimia os russos étnicos em seus protestos pacíficos. A crise estava instalada.[117]

Pouco depois, ainda em abril de 2007, a Estônia foi alvo de intensos ciberataques, que atingiram todo o território do pequeno país báltico. O então ministro da defesa da Estônia, Jaak Aaviksoo, afirmou:[118]

> The attacks were aimed at the essential electronic infrastructure of the Republic of Estonia," "All major commercial banks, telcos, media outlets, and name servers — the phone books of the Internet — felt the impact, and this affected the majority of the Estonian population. This was the first time that a botnet threatened the national security of an entire nation (AAVIKSOO, 2007).[119]

De fato, muito como imaginamos no primeiro capítulo, a infraestrutura essencial de funcionamento da Estônia é uma das mais conectadas ao ciberespaço do mundo. O país chegou

---

[116] MANNESS, Ryan. Cyber policy as a source of power. Russia in Cyberspace. London. 2015. P. 86.

[117] The Guardian. Protest by Kremlin as police quell riots in Estonia. 2007. Disponível em: https://www.theguardian.com/world/2007/apr/29/russia.lukeharding

[118] Wired. Hackers take down the most wired country in Europe. 2007. Disponível em: https://www.wired.com/2007/08/ff-estonia/

[119] Nossa tradução: Os ataques visavam a infra-estrutura eletrônica essencial da República da Estônia "Todos os principais bancos comerciais, telas, meios de comunicação e servidores de nomes - os telefones da Internet - sentiram o impacto e isso afetou a maioria do estoniano população. Esta foi a primeira vez que uma botnet ameaçou a segurança nacional de uma nação inteira

a ser conhecido como E-Stonia, termo em referência à hiperconectividade do país.[120] Botnets poderosas realizavam ataques DDoS incessantes, derrubando *websites* governamentais, serviços de fornecimento de internet e até mesmo o funcionamento de caixas eletrônicos bancários. O Hansabank, o maior banco do país, teve de paralizar as operações online. Os ataques DDoS, realizados de maneira parecida com os do caso do GitHub chinês, "partiam de várias partes do mundo"[121], e atribuir os autores do ciberataque seria difícil, provar estas atribuições, mais ainda. Entendendo como uma botnet funciona, sabemos que os computadores atacando Tallinn eram zumbis, sendo controlados por um indivíduo ou grupo de hackers. Por vezes, websites de figuras governamentais, como do presidente, eram invadidos e tinham seu texto e imagens trocadas com figuras que denegriam ou atacavam a imagem de importantes políticos do país.[122]

Os ataques cibernéticos vieram em meio a uma crise político-diplomática entre russos, a Rússia e a Estônia. O próprio conteúdo das mensagens passadas pelos hackers indicava que russos estavam por trás das ações na Estônia, muito impulsionados pelo tratamento para com a minoria étnica no território. Enquanto que não será possível atribuir conclusivamente as ações ao Kremlin, é clara a relação entre as reclamações de Moscou e as ações no ciberespaço. A utilização das botnets por atores não conectados ao Kremlin, como vimos anteriormente, é uma parte do arsenal estratégico de *cyberwarfare* russo.

Neste caso, os ataques cibernéticos causaram um certo dano psicológico à nação de pouco mais de 1 milhão de habitantes, mas a efetividade da ação é compreendida ao entendermos como a Rússia tem a intenção de manter sua influência em seu exterior próximo. A Estônia tem uma grande população russa, é um Estado que fez parte da União Soviética, e recentemente se tornou linha de frente da OTAN, onde a organização realiza variados exercícios militares, que são muito criticados por Moscou como atos imperialistas e expansionistas.[123] Neste caso, a Rússia viu nos ciberataques como uma maneira de se impor, e efetivamente demonstrar como pode e irá afetar a vida cotidiana em Tallinn. De fato, pouco efeito político surtiu deste ataque, mas o ato foi uma grande flexibilização das capacidades de Moscou em agir em seu exterior próximo de maneira ameaçadora. Em essência, esta foi uma das primeiras ações de ciberguerra, e pareceu como um exercício de teste para o Kremlin. A um custo mínimo, já

[120] E-Stonia. Termo utilizado pelo governo da Estônia. Mais informações em: https://e-estonia.com/
[121] CONNELL, Michael. Russia's approach to cyberwarfare. London. 2017. P 14.
[122] BBC. How a cyber attack transformed Estonia. 2017. Disponível em: http://www.bbc.com/news/39655415
[123] The Guardian. NATO moves to bolster eastern European defences against Russia. 2014. Disponível em: https://www.theguardian.com/world/2014/apr/01/nato-eastern-europe-defences-russia-putin-crimea

que a conexão é complexa de se comprovar, a Rússia relembrou seu desafiador vizinho báltico de que vive ao lado de um gigante.

4.3.1 *Cyberwarfare* convencional?

Em 11 de agosto de 2008, cerca de um ano após os eventos na Estônia, O Ministério de Relações Exteriores da Georgia, através de seu website reserva, hospedado em servidores nos Estados Unidos, anunciou:[124]

> A cyber warfare campaign by Russia is seriously disrupting many Georgian websites, including that of the Ministry of Foreign Affairs. If you cannnot access official Georgian government websites, please go to the following sites for the latest official Government of Georgia news […] (GOVERNO DA GEÓRGIA, 2008).[125]

A acusação do governo da Georgia de que os russos conduziam uma campanha de ataques cibernéticos veio em meio à uma das maiores crises internacionais do século XXI. A Guerra da Georgia muito se deu pela inclinação do então presidente Mikheil Saakashvili em se alinhar ao pensamento pró-ocidente, e pela forma como conduzia a situação das repúblicas separatistas da Ossétia do Sul e da Abhkazia, ambas pró-Kremlin. Em 7 de agosto, a Georgia invadiu o território da Ossétia do Sul, controlado por separatistas, em parte. Em 8 de agosto de 2007, tropas russas, em grande escala, invadiram a Georgia pelo chão, ar e mar.[126] Para Mcconell e Vogler:

> As Russian military forces moved into South Ossetia, a slew of DDoS attacks took down Georgia's networks, cutting off government communications and defacing government websites. Georgian banks, transportation companies, and private telecommunications providers were also attacked, disrupting services. On the day the war started, Russian hacktivist websites, such as stopgeorgia.ru, provided lists of Georgian sites to attack, along with instructions, downloadable malware, and after-action assessments. This opened up a new avenue as far as anonymity was concerned. Theoretically anyone, anywhere in the world sympathetic to Russia, or against Georgia, could contribute to the attacks (MCCONELL, 2017, p. 14).[127]

---

[124] Ministério das Relações Exteriores da Georgia. 2008. Disponível em: http://georgiamfa.blogspot.com.br/2008/08/cyber-attacks-disable-georgian-websites.html

[125] Nossa tradução: Ataques da guerra cibernética pela Rússia derrubam websites do governo da Geórgia; Governo da Geórgia estabeleceu sites alternativos:
Uma campanha de guerra cibernética da Rússia está perturbando seriamente muitos sites na Geórgia, inclusive o do Ministério dos Negócios Estrangeiros. Se você não pode acessar os sites oficiais do governo da Geórgia, acesse os seguintes sites para as últimas notícias oficiais do Governo da Geórgia

[126] DailyMail. Georgia "overrun" by Russian troops. 2008. Disponível em: http://www.dailymail.co.uk/news/article-1043236/Georgia-overrun-Russian-troops-scale-ground-invasion-begins.html

[127] Nossa tradução: À medida que as forças militares russas invadiram a Ossétia do Sul, uma série de ataques DDoS derrubaram as redes da Geórgia, cortando as comunicações do governo e desfigurando os sites do governo. Os bancos georgianos, as empresas de transporte e os provedores privados de telecomunicações também foram atacados, interrompendo os serviços. No dia da guerra, os sites de hackers russos, como o stopgeorgia.ru,

Como colocado pelos autores, de fato, enquanto as tropas russas avançavam sobre o território da Geórgia, rumo à Tbilisi, poderosos ataques cibernéticos afetaram boa parte dos serviços conectados à internet ou ao ciberespaço em todo o território. Com o objetivo de deturpar a comunicação entre os órgãos governamentais e a população, os ataques vinham em conjunto aos ataques militares convencionais, realizados durante a invasão russa. Este fato nos permite realizar uma contextualização entre a doutrina militar russa de 2010, já observada aqui, e as ações das tropas militares russas na Guerra da Geórgia, dois anos antes. Na doutrina, é publicamente colocado que as forças armadas russas buscariam uma maior atuação cibernética para facilitar e/ou viabilizar o uso de estratégias militares convencionais. A doutrina aplicou o que havia aprendido na prática. Ataques cibernéticos afetaram a Geórgia até mesmo meses antes da guerra, e o uso de ataques específicos em alvos que logo depois seriam atacados por forças convencionais facilitavam as operações militares. O Kremlin se negou a confirmar qualquer participação na campanha cibernética, mas a conexão é óbvia, e as acusações do governo da Geórgia tinham fundamento.

Neste contexto, necessitamos entender a importância do evento. Pela primeira vez, uma operação cibernética precedia uma guerra convencional, então promovendo o *cyberwarfare* como uma importante ferramenta para atingir determinados objetivos. Até mesmo para mudar uma guerra. Ainda que como posto por McConnell, a conexão entre os hackers e o governo poderia ser relativa, devido novamente, ao processo de utilização de atores privados para atingir objetivos do Estado, muito como na Estônia, desta vez os ataques eram direcionados em clara cooperação com ações militares convencionais, o que indica, no mínimo, algum tipo de contato entre os agentes do ciberespaço e o alto comando militar russo.

Aqui, observamos, portanto, como a Rússia passou a entender o ciberespaço como mais um dos fatores de guerra, como a força aérea ou as forças navais. Neste cenário, houve a percepção de que as operações cibernéticas poderiam ser utilizadas sempre que possível, já que a relação custo-efeito seria vantajosa. Em essência, o Kremlin havia entendido que as operações cibernéticas eram uma ferramenta de política externa.

4.3.2 Cyberguerra, na prática

forneceram listas de sites georgianos para atacar, juntamente com instruções, malware para download e avaliações pós-ação. Isso abriu uma nova avenida no que diz respeito ao anonimato. Teoricamente, qualquer um, no mundo simpatizante da Rússia ou contrário à Geórgia, poderia contribuir para os ataques.

Anteriormente, observamos as ações de hackers que invadiram o sistema de distribuição de energia elétrica na Ucrânia e deixaram boa parte da população sem acesso à luz em um ato eficiente, inovador e assustador. Quando as luzes se desligaram em Kiev, no ataque cibernético de 2015, a ação não era um fato isolado, mas sim uma parte de um contexto muito mais complexo. Em 2014, mais de um ano antes destes eventos, Vladimir Putin pediu autorização ao congresso para uma intervenção militar na Crimeia, região que pertencia à Ucrânia. O pedido foi feito em 1 de março, mas desde 20 de fevereiro, tropas russas, inicialmente sem identificação em seus uniformes, ocuparam o território da Crimeia.[128] A Crimeia é uma importante região historicamente relacionada à Rússia, e com uma população de maioria étnica russa, ao contrário do resto da Ucrânia. Além disso, a região hospeda uma importante base naval russa, que dá importante acesso ao mar negro. Quando o presidente aliado de Moscou, Viktor Yanukovich, foi retirado do poder pelo parlamento em meio à massivos protestos contra o presidente e de cunho pró-União Europeia, a Rússia percebera que um importante aliado poderia virar um inimigo, e necessitou garantir a integridade da maioria russa e manter o importante território estratégico sobre controle. A ocupação da Crimeia não foi violenta, apenas com poucos episódios de casos isolados, e em 18 de março de 2014, após processo de votação local e pedido de ascensão, a Crimeia era uma parte da Federação Russa.[129]

A anexação da Crimeia foi um ato histórico de extrema importância. Anexações são raras, não acontecem a todo momento nas relações internacionais. Apesar de ela ter sido sem violência, os protestos e a crise política interna na Ucrânia se intensificavam. No leste, apoiadores de Yanukovych, que está em exílio em Moscou, buscavam lutar contra o que chamavam de golpistas e retomar o território, estabelecendo territórios independentes, possivelmente com o desejo de ter o mesmo destino da Crimeia, e se juntar à Federação Russa. De fato, em Donetsk e Luhansk, as coisas se tornaram violentas.[130] Grupos armados de agora rebeldes ucranianos buscavam a independência do governo que acabara de tomar o poder, e declararam esta em meio a tensões que só aumentavam. O governo da Ucrânia agiu, e os separatistas pró-Rússia responderam com fogo. A guerra era uma realidade.

O conflito se desenvolveu e novamente, tropas russas foram envolvidas no processo. O ocidente dizia que a Rússia havia invadido a Ucrânia. De fato, militares russos agiram na

---

[128] Revista Veja. Ucrânia diz que 30.000 soldados russos ocupam a Crimeia. Disponível em: http://veja.abril.com.br/mundo/ucrania-diz-que-30-000-soldados-russos-ocupam-a-crimeia/

[129] Para entender melhor: Forbes: One year after Russia annexed Crimea, locals prefer Moscow to Kiev. 2015. Disponível em: https://www.forbes.com/sites/kenrapoza/2015/03/20/one-year-after-russia-annexed-crimea-locals-prefer-moscow-to-kiev/

[130] BBC. Heavy fighting rages near Donetsk. 2015. Disponível em: <http://www.bbc.com/news/world-europe-32988499>.

Ucrânia apoiando os grupos separatistas, mas após as sanções econômicas e o esfriamento dos embates, a guerra esfriou. O clima ainda era de tensão, e apenas um cessar-fogo foi atingido, e ainda dura. O conflito armado poderia ter cessado, mas a tensão dominava o ar no leste da Ucrânia. Mais de uma vez, os russos cortaram a distribuição de gás natural para a Ucrânia, que é essencial para a calefação no frio inverno do leste europeu, afirmando que os ucranianos não estariam pagando as contas. Aqui, a Gazprom estava sendo utilizada como uma resposta às sanções econômicas impostas pelos Estados Unidos e União Europeia pela atuação russa no conflito da Ucrânia. Essencialmente, os dois países passaram a estar em um conflito não-anunciado, quase que de impossibilidade de coexistência. A energia é uma importante arma russa, assim como as capacidades cibernéticas. De fato, após o cessar-fogo de 2014, a Ucrânia foi alvo de inúmeros ataques cibernéticos.[131] Sistemas financeiros, sistemas de transporte, sistemas de identificação, internet, serviços elétricos, serviços hospitalares e de distribuição de água foram todos afetados por algum tipo de ação ofensiva no ciberespaço em algum momento, e o país sofre para manter a estabilidade da sociedade em meio à pressão de Moscou, dos separatistas do leste, e de fortes ataques à infraestrutura básica do país. Em junho de 2017, o governo da Ucrânia afirmou que os serviços de segurança da Rússia estavam envolvidos em ciber-ataques recentes ao país. Kiev afirma que a Rússia conduz uma "guerra híbrida" contra o país.[132]

De fato, as ações na Ucrânia foram realizadas de uma maneira extremamente consistente e eficiente. O *malware BlackEnergy* foi utilizado com perfeição, prejudicando a acessibilidade de instituições ucranianas ao ciberespaço.[133] Em uma guerra que se tornou silenciosa, o Kremlin viu em ações no ciberespaço como uma importante forma de se fazer presente e aumentar sua influência. Recentemente, hackers russos derrubaram sistemas elétricos na Ucrânia, um ato sem precedentes na história. Em verdade, bancos, hospitais e aeroportos foram atingidos também, e hoje, o funcionamento destas importantes infraestruturas está em sério risco na Ucrânia. A crise é contemporânea, e não está perto do seu final, ao que parece. A lição que parece ficar é de os russos operacionalizaram efetivamente suas operações ofensivas no ciberespaço. Se importantes técnicas menos sofisticadas, como comprar anúncios, para influenciar a opinião

---

131 Reuters. Ukraine hit by 6,500 hack attacks, sees Russian cyberwar. Disponível em: <https://www.reuters.com/article/us-ukraine-crisis-cyber/ukraine-hit-by-6500-hack-attacks-sees-russian-cyberwar-idUSKBN14I1QC>

132 FT. Ukraine's security chief accuses Russia of waging hybrid war. Disponível em: <https://www.ft.com/content/789b7110-e67b-11e3-9a20-00144feabdc0>

133 WELIVESECURITY. Blackenergy strikes again. Disponível em: https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/

pública e ter o apoio de uma grande e hábil comunidade de hackers é importante para se atingir alguns objetivos, o Kremlin mostrou que seus agentes também poderiam atuar ofensivamente como o governo bem desejar. A intervenção na Ucrânia parece servir de campo de teste para os serviços de operações cibernéticas russas, e demonstram como a administração passou a confiar neste tipo de estratégia.

Enquanto que o conflito na Geórgia foi um marco entre a convergência das operações cibernéticas com as operações militares convencionais, o atual conflito na Ucrânia é um grande marco para a promoção do ciberespaço para uma real zona de conflito, influência e poder. Ao atacar as infraestruturas básicas da sociedade, os hackers atingem não somente os governantes do inimigo. A população fica sem energia, sem transporte, sem internet. O caos social é quase que inevitável. Os efeitos de ataques cibernéticos à infraestruturas conectadas ao ciberespaço, como os que acontecem hoje na Ucrânia, são uma perigosa tendência nas estratégias de guerra contemporâneas e futuras. Em Moscou, as autoridades parecem ter entendido como jogar com políticas energéticas e cibernéticas poderiam ser tão efetivo, e enquanto que não podemos saber o futuro, podemos imaginar que conforme as capacidades crescem e na eminência da necessidade de usar estas novas capacidades, o mundo conectado, que, como vimos no primeiro capítulo pode ser boa parte de uma sociedade, ao menos na Ucrânia, está em grave perigo. O Kremlin, parece, efetivamente, ter o entendimento de que as operações cibernéticas são de fato um campo a investir e explorar.

4.3.3 As eleições presidenciais de 2016 nos Estados Unidos

Em 2016, ocorreram as eleições presidenciais dos Estados Unidos, um evento de importância e consequências globais. Entre os candidatos, a favorita, Hillary Clinton pelos democratas, e Donald Trump, pelos republicanos. Trump havia surpreendido boa parte do mundo no desenvolvimento dos eventos desde o anúncio de sua candidatura até a disputada vitória nas preliminares republicanas, e atraía boa parte da atenção da mídia e de estudiosos pela forma como ia realizando sua campanha, e o sucesso deste formato. Trump parecia vir de um mundo de fora da política, com discursos mundanos, sem muito fundamento, e considerado por vezes, agressivo e imoral.[134] No entanto, seu discurso atingia uma grande camada da população norte-americana, que se sente marginalizada pela sociedade, e via em Trump uma

[134] TIME MAGAZINE. Donald Trump attacks Clinton on her marriage. 2016. Disponível em: http://time.com/4515676/donald-trump-hillary-clinton-bill-clinton-marriage/

saída para as políticas de Barack Obama ou Hillary Clinton. Após o fim das preliminares, Clinton, favorita, era alvo de ataques de Trump em variados tópicos, como se tornou natural no processo político americano, no formato de debates. Trump, no entanto, usou e abusou das mídias sociais, como o Twitter, para passar sua mensagem. De fato, o agora presidente utiliza a plataforma de mídia social diariamente, hoje, e mostra de fato a simbiose entre governança e tecnologia (levando em conta que este caso específico é uma simbiose populista, diga-se de passagem).[135]

Neste cenário de inserção tecnológica na política americana, não foi só o Twitter que se tornou parte importante da vida cotidiana em Washington. Ainda durante o primeiro turno, milhares de *emails* do Comitê Democrático Nacional (DNC, em inglês), o órgão que comanda o Partido Democrata dos EUA, foram vazados através de uma invasão de hackers.[136] Os *emails* continham informações que instalaram uma crise interna no partido, quando votantes de Bernie Sanders perceberam que poderia haver uma conspiração para que Clinton vencesse as preliminares dos democratas. Além disso, a imagem da candidata era afetada negativamente pelo cunho da suposta conspiração. Trump venceu as eleições, por méritos de sua campanha e eleito pelo voto popular, sim. Mas o cenário e contexto em que Clinton se encontrou, enfrentando investigação do FBI e sendo bombardeada pelo escândalo interno dos democratas na internet, dividindo os votos do partido e prejudicando a candidata, foram essenciais para a vitória de Trump, principalmente nos chamados *swing states*[137], onde venceu por pouco, e inesperadamente.[138]

Firmas de segurança cibernética como a SecureWorks, Crowdstrike e ThreatConnect afirmaram que as invasões hackers e os vazamentos de informações do DNC foram realizadas pelos grupos russos *Fancy Bear* e *Cozy Bear*, ambos conectados ao Kremlin[139]. De fato, Clinton e os democratas passaram acusar os russos de interferir diretamente nas eleições. Barack Obama, no último mês de seu governo, disse:[140]

---

[135] Ver mais em: http://www.twitter.com/realdonaldtrump

[136] BBC. 18 revelations from Wikileaks hacked Clinton emails. 2016. Disponível em: http://www.bbc.com/news/world-us-canada-37639370

[137] Swing states: os estados dos Estados Unidos onde as eleições sempre são relativamente muito disputadas, sem um partido claramente favorito, e que, em última instância, acabam por definir o resultado dos pleitos eletivos.

[138] Washington Post. How Trump won the presidency with razor-thin margins in swing states. 2016. Disponível em: https://www.washingtonpost.com/graphics/politics/2016-election/swing-state-margins/

[139] BBC. Bears with keyboards: Russian hackers snoop on West. 2016. Disponível em: http://www.bbc.com/news/world-europe-37409456

[140] Em entrevista. Para ver mais: https://www.theguardian.com/us-news/2016/dec/16/obama-retaliation-russia-hacking-us-election

> I think that there is no doubt when any foreign government attempt to impact the integrity of our elections, that we need to take action. And we will, at a time and place of our choosing. Some of it maybe explicit and publicised, some of it may not be. But Mr Putin is well aware of my feelings about this, because I spoke to him directly about it (BARACK OBAMA, 2016).[141]

O Kremlin negou estar por trás das ações. Até o presente momento, apenas a indicação de Vladimir Putin de que russos patrióticos poderiam ter sido os autores da ação demonstra algum tipo de admissibilidade. De qualquer maneira, a crise estava instalada. Os democratas passaram a atribuir, por vezes de maneira exagerada, boa parte dos problemas de Hillary Clinton à interferência russa nas eleições. Parte da mídia seguiu, e logo o presidente eleito Donald Trump passou a ser acusado de ter recebido ajuda dos russos para se eleger.[142] Entre variadas acusações, a importante figura que emerge é de que hoje, enquanto este trabalho é escrito, uma investigação formal, na figura independente do "conselheiro especial" e ex-chefe do FBI, Robert Mueller, existe, para investigar a suposta interferência russa e a colusão das ações da campanha de Trump e o Kremlin.[143] Por mais que não sejam confirmadas empiricamente e sejam tema aberto para debate conclusivo, as ações de hackers russos, provavelmente ligados ao Kremlin, criaram uma situação muito real nos Estados Unidos. A campanha do presidente está sob investigação, o clima de polarização é alto, e a incerteza é grande.

Os problemas internos e a investigação das autoridades norte-americanas surgem em meio a várias disputas geopolíticas entre Washington e Moscou. A guerra da Geórgia, a guerra na Ucrânia, a anexação da Crimeia, as sanções econômicas, a guerra na Síria e outros desentendimentos colocaram as lideranças russas e americanas em choque por mais de uma vez. Os oito anos do democrata Barack Obama, poderiam se tornar doze ou dezesseis com Clinton. Em Moscou, a tendência de desejar a mudança na administração americana era grande. Quando Donald Trump surgiu como opção, é possível que o Kremlin tenha identificado nele como um cenário menos pior ao que viveria com Clinton, já conhecida de Putin e outras autoridades quando foi Secretária de Estado anos antes. Não sendo este o foco da discussão, o ponto a ser levantado é de que por algum motivo ou outro, parecia haver um sentimento de favorecimento para Trump, por parte dos russos, ao menos. Se ele ganhasse, seria melhor.

---

[141] Nossa tradução: Penso que não há dúvida de que quando qualquer governo estrangeiro tenta impactar a integridade de nossas eleições, precisamos agir. E nós, em um momento e lugar de nossa escolha, iremos agir. Alguns atos talvez sejam explícitos e divulgados, alguns podem não ser. Mas Putin está bem ciente dos meus sentimentos sobre isso, porque eu falei com ele diretamente sobre isso.

[142] POLITICO. All of Trump's Russia Ties. 2017. Disponível em: https://www.politico.com/magazine/story/2017/03/connections-trump-putin-russia-ties-chart-flynn-page-manafort-sessions-214868

[143] NY TIMES. Mueller seeks White House documents related to Trump. 2017. Disponível em: https://www.nytimes.com/2017/09/20/us/politics/mueller-trump-russia.html

Em 31 de outubro de 2017, representantes das gigantes de tecnologia Google, Facebook e Twitter, testemunharam perante o Senado dos Estados Unidos. Os executivos que representavam as companhias afirmaram que enxergam indícios de influência russa nas eleições de 2016. O representante do Facebook, Colin Stretch, afirmou:[144]

> Agentes estrangeiros, escondidos por trás de contas falsas, abusaram da nossa plataforma e de outros serviços de internet para tentar semear divisão e discórdia, e para tentar minar o nosso processo eleitoral. É um ataque à democracia e viola todos os nossos valores (COLIN STRETCH, 2017)

As palavras de Stretch chegam em meio à variadas acusações da tentativa de interferência russa nas eleições e da colusão com a campanha de Trump. De fato, os russos parecem ter enxergado em Trump uma alternativa melhor, e talvez o processo democrático tenha sido violado, e Clinton teria vencido sem os ataques cibernéticos e a "campanha informacional" envolvida. Mas se o envolvimento acusado não pode ser comprovado completamente, e não se sabe qual é a real conexão entre a campanha de Trump e o Kremlin, boa parte destes comentários não passa de especulação, ao menos por agora. O que é importante absorver, no entanto, é que mesmo que indeterminado o grau de participação das agências russas no processo eleitoral norte-americano (que os democratas e boa parte da população acreditam ser alto), as ações promovidas por agentes russos parecem ter efeito grosseiro na política dos Estados Unidos.[145] A polarização entre apoiadores de Donald Trump e democratas se tornou muito grande, e o país passou a viver momentos de crise política interna, também impulsionada pela aparente incapacidade de governar efetivamente do recém chegado à Casa Branca.[146] O ponto, portanto, é que mesmo que Vladimir Putin jamais tenha conversado com Donald Trump em segredo, ações de atores russos, desde hackers obscuros até gigantes de mídia como o canal RT, no Facebook e nas mídias sociais como um todo, gravemente impactaram o debate político americano por estarem direcionando o público à uma temática parcial e por vezes até falsa. Parece, de fato, que a própria "intervenção" nas eleições se tornou uma poderosa arma para dividir o país.

Talvez, o efeito das operações cibernéticas seja uma questão de sorte. Mas ao observarmos a história, veremos que não somente nos Estados Unidos os canais de mídia russos,

---

[144] Em testemunho ao Senado dos Estados Unidos.

[145] BI. Explanation to polarization on US politics. 2017. Disponível em: http://www.businessinsider.com/sociology-explains-polarization-politics-2017-3

[146] The Independent. Trump's approval rating falling. 2017. Disponível em: http://www.independent.co.uk/news/world/americas/us-politics/trump-approval-rating-polls-popularity-latest-fall-states-a7995201.html

conectados ao Kremlin, promoveram algum tipo de debate político incorreto ou então bem parcial. Em essência, para entendermos a gravidade da questão, o Twitter anunciou, em 26 de outubro de 2017, que baniria propagandas pagas advindas do Sputnik e do RT, além de bloquear algumas contas relacionadas aos canais russos, os mesmos que observamos no capítulo 2 como tendo utilizado *bots* para promover debate político na França.[147] Ao observarmos este comportamento, entenderemos que a promoção de Donald Trump, por parte destes canais, não era uma coincidência, mas sim, de fato, uma estratégia advinda da caixa de ferramentas do *cyberwarfare* russo.

Conforme as acusações aos russos evoluem no Senado em Washington, talvez a situação fique mais clara. De qualquer maneira, o fato de que gigantes midiáticos da Rússia consistentemente divulgavam notícias ruins sobre Clinton, em inglês, é real.[148] Além disso, especialistas afirmaram que, realmente, hackers russos invadiram o DNC.[149] Ainda, como vimos no testemunho de executivos, os responsáveis pelas maiores companhias de tecnologia do mundo afirmam que agentes russos agiram para influenciar a opinião pública nas eleições. A constante divulgação de notícias (como na França), a compra de anúncios no Facebook, a organização de eventos inexistentes e as invasões e vazamentos de informações comprometedoras parecem sair direto de um arsenal de guerra informacional. A relação do Kremlin com a questão não é de hoje. As autoridades na Rússia aprenderam logo cedo que teriam de lidar com a informação de uma maneira bem específica, se quisessem governar, como vimos anteriormente. Ainda, Putin sentiu na pele que mesmo com o aparato estatal por trás de si, ninguém poderia fugir das garras da internet ao enfrentar os maiores protestos que a Rússia contemporânea já viu, que em boa parte foram organizados online. De fato, cabe o questionamento, a ser respondido em outro momento: Quantas destas ONGs e indivíduos que organizaram protestos online não eram influenciados por agentes estrangeiros, como parece ser natural no ciberespaço hiperconectado? De qualquer maneira, o Kremlin parece ter aprendido como manusear a questão da informação online muito bem.

A relação de Trump com os russos não é clara, no momento. Por mais que as acusações existam, na visão deste trabalho, é provável que as operações cibernéticas promovidas contra os Estados Unidos sejam esforços não para eleger Donald Trump, o que poderia ser um efeito

---

[147] BBC. Twitter bans RT and Sputnik ads amid election interference fears. 2017. Disponível em: http://www.bbc.com/news/world-us-canada-41766991

[148] RT. Role of Hillary Clinton in Lybia war exposed. 2016. Disponível em: https://www.rt.com/usa/334400-hillary-clinton-libya-role/

[149] The Guardian. DNC email leak: Russian hackers Cozy Bear and Fancy Bear behind breach. 2016. Disponível em: https://www.theguardian.com/technology/2016/jul/26/dnc-email-leak-russian-hack-guccifer-2

agradável, mas principalmente para desviar o debate político, afetar o processo democrático, e em sua essência, dividir o país. Em síntese, se este for o pensamento, a efetividade das ações advindas do ciberespaço foi esplêndida. Os americanos focam boa parte das discussões na mídia, nas conversas sociais e no Congresso em resolver a questão da "interferência russa", e a Casa Branca passa boa parte do seu tempo se defendendo de acusações de conspiração com agentes estrangeiros. Talvez seja este o segredo. Os russos agiram, com suas ações na internet, para aparentemente causar uma divisão no país e desviar o debate, e não para simplesmente eleger Trump por ele ser algum tipo de espião, uma narrativa que mais parece um filme de Hollywood. Em essência, é isto que os americanos, até o momento, falharam em entender. A própria existência da discussão, e ela existe, e é constante e importante no país, mostra o sucesso das operações de desinformação advindas de Moscou. Ainda que a relação entre as autoridades e os hackers seja obscura no presente momento, seria ingênuo imaginar que toda esse confluência de forças não teria no mínimo uma participação estatal, ainda mais observando o histórico interno da Rússia. Efetivamente, a Rússia parece ter afetado com sucesso o processo estadunidense.

4.4 O mundo cibernético de Vladimir

Observamos as operações efetuadas por hackers russos em diferentes tempos e contextos. Em 2007, ainda vivíamos os anos de juventude do ciberespaço, ao menos se considerarmos as analogias modernas à este. Neste mesmo ano, as operações na Estônia são vistas como uma das primeiras interações públicas entre dois grandes atores no ciberespaço, que afetavam diretamente a infraestrutura de um país. Nos próximos anos, o *cyberwarfare* russo parece ter se desenvolvido em uma interessante convergência de operações informacionais sutis e de operações invasivas e com potencial para danificar infraestrutura física e até mesmo ser a causa de atos fisicamente violentos. Quando a Rússia invadiu a Geórgia, em 2008, parecia natural que as forças armadas agissem também no ciberespaço, já que o mesmo se conectou imensamente à realidade humana, como vimos no primeiro capítulo. Em uma situação como a da Ucrânia, a tensão real - onde tiros foram disparados e mortes ocorreram – parece se traduzir no mesmo para o ciberespaço: Várias infraestruturas básicas sendo alvo de ataques cibernéticos, potencializando o clima caótico no país. Em essência, cabe até, em outro momento, analisarmos tanto a efetividade quanto a moralidade deste tipo de operação de guerra ofensiva, visto que envolve uma grandiosa camada de civis. No entanto, o que é importante que percebamos neste momento é a conexão entre a tensão real, e atos mais agressivos no ciberespaço. Parece,

curiosamente, que os dois espaços detêm uma certa sintonia. Na situação dos Estados Unidos, enquanto que muito recente para analisarmos francamente em sua totalidade, já é possível observarmos que Moscou entendeu a situação como uma oportunidade para desempenhar suas técnicas mais leves no ciberespaço. Enquanto que realizou operações agressivas anteriormente, como a invasão dos servidores do DNC, passou a focar na utilização das mídias sociais, incluindo mecanismos legítimos, como a aquisição de anúncios, e de uma campanha informacional, como promover notícias demasiadamente através de seus meios de comunicação em inglês, como o canal RT, assim mostrando uma real capacidade de operacionalizar seus atos de maneira híbrida, como colocaram estudiosos da OTAN.[150]

Assim sendo, Moscou pôde efetivar algum tipo de operação para adquirir algum tipo de vantagem sem disparar um tiro sequer, ou nem mesmo chamar a atenção com atos consideravelmente vistos como "agressivos", como cortar a energia ou desligar sistemas de comunicação. Portanto, é realmente observável este aspecto híbrido do *cyberwarfar*e promovido pelo Kremlin, onde determina o curso e o cunho de suas ações de acordo com a situação que se põe à sua frente, e, quase que inegavelmente, acabou tornando o ciberespaço como uma importante zona do pensamento estratégico da administração de Vladimir Putin, sendo assim, um dos, se não o principal, principais atores no ciberespaço, se tornando assim extremamente influente nesta zona, e consequentemente, no mundo. Em essência, se a ideia da Rússia jamais ter deixado de ser um grande ator internacional, como colocada por Putin em 1999, era algo distante após o fim da guerra fria, a presença russa no ciberespaço garante à Moscou uma *de facto* influência na vida cotidiana global, incluindo no ocidente, ao observarmos a grande conectividade do mundo à rede e entendermos suas características e tendências de hiperconectividade.

No século passado, a Rússia havia passado por intensas crises e longos períodos transitórios. A chegada da administração atual ao poder e a estabilização das questões domésticas, como um todo, permitiram uma maior tranquilidade política em Moscou. Conforme a tecnologia foi avançando, as autoridades russas passaram a compreender como o ciberespaço poderia ser uma importante ferramenta para administrar a influência russa no exterior, seja em seu exterior próximo ou globalmente. Após a estabilização interna, o Kremlin começou a flexionar seus músculos militares. Ainda que por muitas vezes agindo de maneira defensiva, Moscou tomou atitudes consideravelmente ofensivas, como, por exemplo, quando

[150] Mais informações em: https://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0

passou a bombardear os rebeldes sírios e salvou o regime de Bashar Al Assad.[151] Essencialmente, como vimos anteriormente neste capítulo, a questão da grandeza da Rússia não é uma analogia vazia. Para os russos, a Rússia é e sempre será uma superpotência, e agir como tal é motivo para orgulho, e estabilidade. Realmente, com números militares massivos e grande potencial econômico, este país exercer sua influência parece quase que natural. Ainda, cabe observar que por várias vezes atores poderosos como a OTAN mostraram uma certa agressividade à Moscou, país que aparentemente nunca fez parte da ideia de "aliados" que alguns países como os europeus e os EUA dividiram após a Segunda Guerra. A divisão causada pela Guerra Fria ainda é bem real. Em um cenário onde os Estados Unidos e seus aliados se expandem de tempo em tempo, como nos exercícios militares da OTAN na Estônia, logo na porta da Rússia, ou na instalação do controverso escudo de mísseis na Polônia, a estabilidade política no Kremlin passou a ser uma necessidade para não sucumbir à pressão.[152] No ciberespaço, o Kremlin parece ter encontrado uma interessante válvula de escape para exercer seu poder, e até mesmo causar receios e medo em seus adversários.

Neste contexto, os russos, sob pressão, passaram a agir mais e mais dentro do ciberespaço. Ao agirem mais consistentemente e com cada vez mais efetividade, parece que uma mensagem passou a assombrar a mente dos legisladores no ocidente: Podemos deter a Rússia, se necessário? Vladimir Putin anexou a Crimeia, em 2014. Nos anos seguintes, Moscou realizou uma série de operações cibernéticas que danificaram a sociedade ucraniana bem onde mais importa, no conforto e segurança de seus lares, sem sequer disparar uma bala. Na Europa ocidental e nos Estados Unidos, o coração e alma da OTAN, serviços de informação russos constantemente passaram a criar uma campanha de desinformação que, em sua essência, mais parece existir para enfraquecer os adversários políticos que sufocam o Kremlin do que algum plano mirabolante de dominação mundial. Ainda que com um certo grau de exagero em partes, o Kremlin foi acusado de estar conduzindo uma cyberguerra por várias autoridades de países diferentes. Reino Unido, França, Estados Unidos, Ucrânia, Geórgia estão entre alguns dos países que acusaram os serviços de segurança da Rússia de estarem por trás de diversas ações ofensivas no ciberespaço.[153] Mesmo que em alguns casos seja pura especulação, cabe entendermos que o Kremlin parece mesmo ter visto neste tipo de ação uma grande oportunidade de se fazer presente. Devemos levar em consideração que a economia russa não se equipara

[151] BBC. Russia joins war in Syria. 2015. Disponível em: http://www.bbc.com/news/world-middle-east-34416519
[152] RT. Russia will respond to NATO expansion – Putin. 2017. Disponível em: https://www.rt.com/news/392166-putin-stone-nato-expansion/
[153] BBC. Russia causing cyberspace “mayhem” says ex-GCHQ boss. 2017. Disponível em: http://www.bbc.com/news/technology-40557092

com a de seus principais rivais, e o investimento militar consome boa parte desta, devendo ser, portanto, limitado se uma recuperação econômica real é um objetivo. Por exemplo, o orçamento da Defesa na Rússia é cerca de dez vezes menor do que o orçamento de Defesa dos Estados Unidos, e ainda assim, boa parte das autoridades americanas tratam a Rússia como uma grande agressora.[154] Neste cenário, onde existem limites para o número de tanques e bombas da Rússia, o Kremlin enxergou que no ciberespaço, à um custo menor, sua presença poderia ser global. A Rússia, de fato, está em todos os lados no ciberespaço. Parece, se nos permitirmos imaginar, que o próprio sonho de Vladimir Putin, de 1999, se tornou realidade.

A presença russa no ciberespaço não é baseado em desorganização e empolgação pela plataforma relativamente nova. Ao contrário do que suas táticas impõe à quem sofre ataques, os russos parecem ter suas estratégias bem definidas. Ao relembrarmos o *soft power* e o *hard power* cibernético colocados por Nye, poderemos identificar e contextualizar as ações de hackers russos. Quando os *trolls* da Letônia, os *bots* da França e os anúncios em mídias sociais dos EUA se juntam, podemos observar táticas de guerra informacional sutis, que atingem diretamente a opinião pública e, possivelmente, o processo democrático. Este tipo de operação é aplicada por Moscou quando aparentemente as autoridades que tomam as decisões entendem que um cenário de caos interno em determinado alvo seria a melhor, ou única, opção. Moscou não poderia, no momento, e nem quer, colocar tanques em Paris. Mas extremar o debate e apoiar uma candidata que o Kremlin entende que enfraqueceria a França com seu isolacionismo através da promoção e divulgação de opiniões parciais é uma alternativa viável, que pode render grandes frutos. Basta apenas imaginar: Para a Rússia, o que seria melhor? Um Estados Unidos de liderança, forte, e determinado, ou um cheio de problemas internos, discussões, polarização política e incerteza geral? Neste ponto, as ações nas eleições americanas se fazem entender por si só. Não é que Trump seja algum grande amigo de Putin, mas sim o caso de promover um cenário onde não existem ganhadores reais, e sim uma interminável discussão e desunião que podem só ter fim em 2022. Em essência, estas operações buscam, de maneira sutil, afetar o próprio pensamento de cidadãos ao redor do mundo e acabar afetando a sociedade internamente. São operações de relativo *soft power*.

Já quando os tanques invadiram a Geórgia, ou quando os rebeldes pegaram em armas no leste da Ucrânia, as operações seriam diferentes. Ataques DDoS que desabilitam o acesso à internet, invasões cibernéticas de sistemas de distribuição de energia e a utilização de *malware*

[154] CNN. Russia the third largest military spender. 2017. Disponível em: http://money.cnn.com/2017/04/24/news/russia-military-spending/index.html

para debilitar a comunicação são ações impactantes, fortes. Quando ficamos sem energia, principalmente nas regiões mais urbanizadas, a reação é uma mistura de pânico e tristeza. Quando não conseguimos nos comunicar, o desespero parece tomar conta. Ao agir exatamente nestes sentimentos, as operações mais agressivas no ciberespaço afetam o psicológico, possivelmente de toda uma nação, e sistemas de infraestrutura, podendo até mesmo causar danos bilionários. Estas operações, em geral, parecem ser realizadas em cenário agressivo, de guerra. Ainda que os ataques DDoS sejam mais deliberadamente usados, os ataques efetivos à infraestruturas são mais contidos contra países poderosos. Maness afirma que Moscou não utiliza todas as suas ciber-capacidades para evitar retaliações. De qualquer maneira, fica claro que este tipo de operação é uma operação de *hard power*, que se atrela à atividades de guerra convencional, quando possível. Portanto, a evolução do pensamento das autoridades em Moscou não foi somente a de uma inserção rápida, mas também a de toda a construção de uma estratégia bem definida para lidar com situações diferentes. Realmente, o ciberespaço se tornou uma ferramenta de política externa essencial e efetiva no caso da Rússia.

Neste contexto, é essencial também observarmos que os russos não detêm o monopólio das ações no ciberespaço, e nem seriam capazes disto. Como observamos no segundo capítulo, em relação às grandes potências, em geral, todas se inseriram de uma maneira ou outra neste novo contexto, sendo quase impossível para um Estado não estar envolvido, de alguma forma, com o ciberespaço, hoje. Ainda mais, na questão da chamada "interferência", como está sendo discutida hoje nos Estados Unidos, a presença de norte-americanos ou europeus em outros Estados é demasiadamente relevante. Não é de hoje o histórico de interferência estrangeira por parte dos Estados Unidos em outros países. Ainda, na questão da internet e na interferência em processos democráticos, as acusações chegam a ser irônicas para quem observa de perto o comportamento de algumas figuras políticas estadunidenses. Isto fica evidente quando, em maio de 2017, Barack Obama publicou um vídeo em redes sociais declarando seu apoio e instruindo os eleitores franceses para que votassem em Emmanuel Macron.[155] Ainda que não estando em posse de cargo eletivo, o ex-presidente é uma figura carimbada atrelada ao poder de Washington, e aqui, a "interferência" não poderia ser mais clara. Curiosamente, este caso não levantou acusações, não causou furor e nem pânico. Por vezes, a existência da russofobia, termo utilizado por Putin para denunciar uma crescente atitude discriminatória para com russos,

[155] The Guardian. Obama backs Macron in last-minute intervention in French election. 2017. Disponível em: https://www.theguardian.com/world/2017/may/04/barack-obama-backs-macron-in-last-minute-election-intervention

parece ser bem real. O âncora do RT America, Ed Schultz, sobre as investigações de interferência russa, disse:[156]

> We are not propaganda, and we do not take orders from any government entity involving content on RT America. Furthermore, none of the journalists that work at this network have anything to do with any advertising campaign on any social network platform (ED SCHULTZ, 2017).[157]

Schultz, em transmissão do canal, ainda comentou sobre o "histórico de intervenção estrangeira" dos Estados Unidos. Em essência, Schultz não parece estar errado. Os americanos realmente agem como hipócritas ao ignorarem suas próprias ações, mas a imparcialidade do homem que afirmou isto também é questionável. O RT é uma importante ferramenta de propaganda russa, e como observamos, já foi utilizado para atingir determinados objetivos do Kremlin.

Hoje, todos os grandes atores geopolíticos globais também estão agindo no ciberespaço. Como observamos em Maness, os Estados Unidos, China e Rússia são os atores mais poderosos no ciberespaço, e no caso dos EUA, por exemplo, as capacidades ofensivas parecem ser até melhoras que as russas. Por quê, então, toda essa especulação de que Moscou estaria conduzindo uma ciberguerra, ou acusações de que Moscou estaria interferindo em países pelo mundo todo, principalmente se os americanos e chineses tem uma capacidade cibernética relativamente igual ou melhor em certos pontos do que os russos? Como colocado por Malcolm Nance (2016, p.21), a resposta passa muito pela forma como as operações cibernéticas foram teorizadas e aplicadas em cada país. Os Estados Unidos, em suas operações cibernéticas, agem para operacionalizar e criar armas de alta qualidade, precisas, específicas, que devem ser testadas para então serem aplicadas. O caso do Stuxnet e o ataque às centrifugas nucleares iranianas é um ótimo exemplo. Os chineses, para Nance, enquanto que ainda detém uma certa agressividade e hibridez comparativa à dos russos, foca boa parte de seus recursos e operações em ganhos econômicos, como em operações de espionagem industrial, e de controle interno, como no caso do firewall. Já os russos passaram a utilizar as operações cibernéticas como uma alternativa viável para atingir objetivos geopolíticos. E não somente isto, Moscou passou a enxergar o ciberespaço como uma importante ferramenta estratégica, e portanto desenvolveu

[156] RT. Ed Schultz comments on investigations. 2017. Disponível em: https://www.rt.com/usa/408527-ed-schultz-russia-investigation-alleged-meddling/

[157] Nossa tradução: Não somos propaganda, e não recebemos pedidos de qualquer entidade governamental envolvendo conteúdo na RT America. Além disso, nenhum dos jornalistas que trabalham nesta rede tem qualquer coisa a ver com qualquer campanha publicitária em qualquer plataforma de rede social.

estratégias específicas para lidar com variados tipos de situações, não se limitando a agir somente quando necessário ou para atingir alvos muito específicos. Isto foi, como observamos, muito potencializado pela maneira como a própria sociedade russa se desenvolveu nos últimos anos, os anos em que o ciberespaço e a internet também se tornaram protagonistas da vida de boa parte do mundo. No contexto da chegada de Vladimir Putin ao poder e o desenvolvimento das relações internas, os *hackers* russos passaram a atuar, por vezes, em uma interessante parceria entre o público e o privado. Assim sendo, as políticas do Kremlin criaram uma boa margem para impulsionar a Rússia como um dos principais atores no ciberespaço.

Neste cenário, a Rússia passou a se tornar proponente no ciberespaço. Em essência, parece que *hackers* russos, estejam eles conectados ao Kremlin ou não, aprenderam como operacionalizar suas diversas ações efetivamente, e parecem estar delineando as linhas do que é ou não aceitável nas relações internacionais do ciberespaço. De fato, este é um campo muito inexplorado nas relações internacionais, e por isso as ações do Kremlin parecem ser chocantes aos olhos de muitos. Porém, para Moscou, a utilização do ciberespaço como um viabilizador de seus objetivos se tornou normal. Tanto para se proteger domesticamente quanto para exercer seu poder global à um custo político e financeiro baixo, a Rússia passou a efetuar as operações mais inovadoras e efetivas de um Estado no ciberespaço. Este cenário está em constante transformação e é, para muitos, uma incógnita. Mas até o presente momento, se quisermos buscar os ganhadores nas disputas dentro do ciberespaço, devemos olhar para Vladimir Putin e seus colegas, que parecem ter aprendido como agir efetivamente neste novo contexto.

5 Considerações Finais

Primeiramente, observamos como a revolução tecnológica pela qual passamos se tornou parte essencial da vida cotidiana. A utilização da internet e a digitalização dos mais variados setores dentro de uma sociedade contemporânea se tornou uma tendência global, afetando a maioria dos seres humanos vivos. A ascensão do ciberespaço nas últimas décadas ganhou força recentemente, e boa parte do mundo desenvolvido está envolvido pela camada invisível de elétrons que nos cercou. Ainda, observamos como o ciberespaço é essencial para a nova realidade de alguns serviços essenciais da sociedade, como por exemplo, o cadastramento de cidadãos, o processo eleitoral e a distribuição de energia elétrica. Em sequência, entendemos como as características específicas do ciberespaço, sendo relevante citar a propensão à anonimidade, a velocidade da ação-reação, a aparente falta de fronteiras (ao menos como as conhecemos originalmente) e a característica anárquica da internet, são tanto um processo essencial para a sociedade humana contemporânea desenvolver quanto um perigo para determinadas situações e atores, sendo amplo o espaço para criminosos e outros atores interessados efetuarem ações danosas à indivíduos, empresas ou governos. Por ser um evento recente, a ascensão do ciberespaço, e da internet, ainda existem inúmeras questões a serem definidas, como a regulamentação (ou não) do mesmo e entender melhor os próprios limites de onde esta tecnologia pode chegar. Enquanto isso, governantes e cidadãos do mundo todo vão se adaptando conforme a plataforma vai se desenvolvendo.

Neste cenário, vimos que os Estados-Nações são atores que rapidamente procurariam explorar o ciberespaço, de uma maneira ou de outra. De fato, o Estado, como um todo, é um dos principais desenvolvedores desta plataforma, já que ela é muito benéfica em algumas questões. Logo, sistemas essenciais controlados ou regulamentados pelos Estados passariam a utilizar o ciberespaço como plataforma anexa ou até mesmo principal. Em essência, parece que sistemas conectados à internet e ciberespaço são de fato mais eficientes, e a tendência é de que o processo se intensifique. Podemos observar isto bem ao analisarmos a situação da Estônia, onde o pequeno país báltico se tornou um dos principais proponentes da digitalização da governança e de sistemas úteis, mesmo tendo sofrido com ataques cibernéticos. Ainda, cidades inteligentes e redes elétricas inteligentes são uma realidade: É extremamente útil e eficiente o processo de digitalização da distribuição de energia, transporte, cadastro, entre outros. Por isso, países desenvolvidos como os Estados Unidos, Holanda e Alemanha passaram a cada vez mais utilizar tecnologias novas conectadas ao ciberespaço para melhor evoluir seus sistemas de

infraestrutura. As *smart grids* não só são extremamente eficientes, mas também são uma tendência, assim como os outros processos eletrônicos que se conectaram ás infraestruturas recentemente.

Em contrapartida, logo pudemos entender que por mais que os benefícios sejam imensos, o ciberespaço é uma plataforma muito recente, com regulamentação inexistente, fraca ou ineficiente, e que deixa brechas que promovem uma certa fragilidade na questão da segurança cibernética. Além disso, a especificidade da plataforma mais relevante nesta questão parece ser a de que um usuário ou um grupo de usuários bem capacitados pode ter um efeito grandioso, onde as armas mais poderosas não parecem ser exclusividade de governos estabelecidos, como acontece na era das armas nucleares. No ciberespaço, a diversidade de atores hábeis parece ser muito maior, e os perigos e propensão ao caos também. Ainda, estes atores estão protegidos, por vezes, por uma camada de anonimato que não é comum ao que operações de guerra ou simplesmente ofensivas apresentaram na história humana, tornando portanto este espaço ainda mais complexo, onde é difícil apontar a culpabilidade e definir com total certeza quem promoveu determinadas ações, assim como onde e quando.

Observamos que os Estados logo entenderam isto, e passaram tanto a utilizar o ciberespaço para seu benefício e proteção quanto para operacionalizar ações ofensivas para atingir variados objetivos. Logo, atividades como as reveladas por Edward Snowden se tornariam tanto um choque quanto algo cotidiano para muitos, já que governos mundo afora passaram a espionar em cidadãos através da internet ou de serviços de comunicação. Em essência, a espionagem ou até mesmo o controle da internet como no caso chinês se apresentam como necessidades para os governos manterem algum nível, nem que mínimo, de controle sobre as informações no ciberespaço, que hoje, afetam diretamente a vida fora do ciberespaço. Isto é facilmente compreendido quando observamos o caso das eleições norte-americanas, onde vazamentos de *emails* privados denegriram a imagem da então candidata à presidência Hillary Clinton. É observável que ações no ciberespaço, envolvendo informações existentes nele, poderiam ser danosas à reputação de políticos ou até mesmo de qualquer cidadão, podendo até mesmo afetar a governabilidade ou estabilidade política e social em um país, passando ser necessária a presença estatal neste meio.

Além destes fatos, as relações interestatais também estão ligadas ao ciberespaço, e armas cibernéticas podem ser utilizadas por um ator estatal contra o outro em determinadas situações. Como no caso das centrífugas iranianas e da rede elétrica ucraniana, Estados foram alvos de ataques cibernéticos em infraestruturas essenciais, causando danos bilionários. Neste

contexto, a cibersegurança parece ser uma necessidade prioritária. Além de se defender, os Estados mais poderosos passaram a observar como poderiam atingir determinados objetivos com operações no ciberespaço, que em geral, parecem ter um custo menor do que outras operações, como as militares convencionais ou até mesmo, por vezes, sanções econômicas que tem um grande custo diplomático. Assim sendo, os Estados passaram a securitizar a questão do ciberespaço e a planejar e operacionalizar ações efetivas contra outros atores importantes dentro desta plataforma, mas com efeitos no mundo real. Assim sendo, a ascensão do ciberespaço é uma realidade nas relações internacionais, onde atores estatais constantemente buscam ampliar suas capacidades técnicas para obter vantagens estratégicas.

Na sequência, passamos a entender que os Estados, neste cenário, preparam e desenvolvem seu *cyberwarfare* para situações diversas. Ao observarmos o caso do firewall chinês, passamos a compreender como entes governamentais passaram a lidar de maneira minuciosa com a informação online. Os chineses passaram a controlar todo tipo de influência estrangeira em sua internet, até mesmo redefinindo o conceito de internet para se adaptar à sua "soberania na internet". É essencial entendermos que as operações informacionais parecem ser naturais hoje em dia para as grandes potências, e os casos apresentados por Edward Snowden e o caso chinês analisado neste trabalho demonstram uma tendência generalizada de que o Estado deve desempenhar um papel importante no controle e disseminação de informação online.

Neste cenário, observamos como as armas cibernéticas utilizadas por atores, estatais ou não, podem manusear a informação para melhor atingir determinados objetivos. Os chineses buscam controlar seu ciberespaço, mas não são os únicos atores que lidam com a informação na internet. Vimos como a Rússia parece utilizar *bots* e *trolls* para desviar o debate público em outro país, assim como foi possível observar que grupos políticos domésticos também agem no ciberespaço ao observarmos o caso dos *bots* no debate político brasileiro nos anos recentes. Em essência, atores variados, incluindo os Estados, parecem interagir com a informação no ciberespaço, e então moldar, alterar ou produzir informações que sejam satisfatórias para atingir objetivos políticos internos e externos, dependendo da situação.

Ainda, passamos a entender que as operações no ciberespaço aparentemente se dividem em duas, onde as questões informacionais mais sutis são um lado, e o poder agressivo de ataques de hackers ou ações do tipo são o outro. De fato, enquanto manuseiam a informação como uma arma sutil, os atores no ciberespaço também operacionalizam ações agressivas como os ataques DDoS ao Github, o *malware* que infectou as centrífugas iranianas e as APTS de aparente origem

chinesa que afetaram sistemas governamentais americanos por mais de uma década. Este tipo de ação é mais impactante, e demonstra uma clara presença de atores poderosos com intenções bem definidas no ciberespaço. No cenário das relações internacionais, é importante entendermos que estas operações agora são parte do arsenal da maioria dos países desenvolvidos, e no mínimo, ter um conhecimento destas é importante para se defender, na visão de um ator estatal. Portanto, os Estados, sendo os principais atores no sistema-mundo e no ciberespaço, passaram a investir uma grande quantidade de recursos em tecnologias e operações cibernéticas, seja para se proteger ou para atingir objetivos estratégicos. Assim sendo, o ciberespaço se tornou importante campo de influência, ação e planejamento para os Estados-Nações, que buscam constantemente desenvolver suas capacidades cibernéticas.

Entendemos, portanto, como se daria, através das mais variadas ações, o cenário de uma possível guerra cibernética, e que armas seriam utilizadas nesta. Para entendermos as capacidades cibernéticas dos principais atores internacionais, é importante que observemos as operações informacionais citadas anteriormente, sua relevância, e seus efeitos variados. Como posto por Libicki, a difusão de informações é um processo essencial nos processos de guerra cibernética, visto que o ciberespaço é essencialmente composto por informação e hardware. Assim sendo, a habilidade de hackers em manipular a informação e a mente das pessoas através da engenharia social é essencial para o sucesso de muitas das operações cibernéticas. Além disso, o uso da informação como arma cibernética é quase redundante, já que é claro o efeito negativo de divulgar e promover notícias e mensagens falsas, podendo desviar imensamente o debate público em uma sociedade da realidade. Na sociedade contemporânea, por influência do ciberespaço, a informação é essencial para todos, desde um cidadão comum até poderosos governantes de potências globais. Além disto, a informação está conectada a importantes fatores econômicos, como o mercado de ações, e ao funcionamento de infraestruturas essenciais, como na distribuição de energia, assim sendo, a capacidade de manusear informações é essencial para compreendermos o poder cibernético de atores internacionais.

Além disto, vimos, como colocado por Nye, que o poder cibernético deriva da habilidade e capacidade de um ator ter seus objetivos atendidos através do uso de recursos informacionais conectados eletronicamente. Essencialmente, Nye nos mostra que o poder cibernético advém da habilidade de manusear a informação sutilmente (*soft power*) e da capacidade de utilizar informação para produzir armas efetivas que afetam até mesmo espaços fora do ciberespaço, por vezes (*hard power*). O poder cibernético dos atores passa muito pela capacidade de induzir ações em outros atores, controlar sua agenda de alguma maneira e, ou,

influenciar a opinião dos outros atores para que ignorem certas estratégias que seriam danosas ao autor das ações. Além disto, é importante lembrar que o poder cibernético também varia de recursos humanos e da capacidade de investimento em educação e em infraestrutura. Portanto, o poder cibernético estatal é, de fato, o maior poder cibernético devido ao de facto monopólio estatal de angariar recursos financeiros, humanos e estruturais em grande escala. Ainda, como vivemos no mundo real, a legitimidade estatal de impor regulamentações e leis que podem afetar diretamente as operações cibernéticas, como prender um hacker, por exemplo, tornam estes atores como os mais influentes, assim como é a vida no mundo fora do ciberespaço. Porém, devido às interessantes características do ciberespaço, a difusão de poder dentro deste é muito maior. Como posto por Nye, uma pequena porcentagem de ciber criminosos é identificada e capturada, sendo o ciberespaço um grande campo de atuação para atores com más intenções. Portanto, mesmo que o Estado detenha o maior poder cibernético, ainda existem outros atores hábeis que podem causar dano significativo a estes próprios poderosos atores estatais.

A assimetria do poder cibernético em comparação a outros poderes é importante para entendermos o poder cibernético como um todo. Como diversos atores podem agir no ciberespaço, como um hacker solitário em seu computador, os Estados com infraestrutura mais conectada ao ciberespaço podem sofrer demasiadamente com ataques partindo de diversos locais, o que pode levar à pânico generalizado. As vulnerabilidades cibernéticas são essenciais no processo do poderio cibernético, pois, em essência, se algo não está conectado ao ciberespaço, não pode ser diretamente atacado por algo advindo deste mesmo ciberespaço. Logo, nações mais desenvolvidas tecnologicamente, como vimos em Maness, são um alvo maior e mais fácil de diversos atores cibernéticos. A ciber dependência é algo crítico se pensarmos em segurança, e em conjunto com as capacidades ofensivas e defensivas formam o conjunto de capacidades cibernéticas que podem definir o poder cibernético de determinado ator. Assim, observamos que países como os Estados Unidos e Alemanha, mesmo que poderosos ofensivamente, podem ser alvo de ações de hackers por estarem demasiadamente conectados ao ciberespaço, deixando lacunas e brechas de segurança. Porém, a efetividade das operações cibernéticas, como vimos anteriormente, não são factíveis somente se pensarmos nas capacidades ofensivas, mas também na capacidade de se manusear a informação e poder, a um nivel estatal, regulamentar o ciberespaço.

Por isso, neste cenário, países como a Rússia e a China parecem ser atores extremamente capazes. A Rússia é vista como um dos principais atores cibernéticos não só devido à suas

capacidades ofensivas, mas também à capacidade regulamentar e controlar o fluxo de informações em sua internet, assim como efetivamente manusear a informação para que o que chegue aos olhos e ouvidos de quem importa seja relativamente concordante com os desejos da administração estatal. Ainda, as características internas da sociedade russa e como ela se desenvolveu acabaram por criar um cenário onde atores não estatais podem agir em convergência com atores estatais, dando assim ao país uma grande capacidade de mobilização no ciberespaço, e ainda, como colocado por Nye, estes atores não-estatais podem servir para que a culpabilidade do ator estatal jamais seja conclusiva, apresentando portanto um custo baixíssimo em termos políticos e diplomáticos. Por fim, a estrutura tecnológica na Rússia não é tão avançada como em alguns outros países, a tornando um alvo menos óbvio e mais difícil de ser afetado efetivamente por operações no ciberespaço. Em combinação, estas características demonstram um grandioso poder cibernético emanando de Moscou.

Para efetivamente compreendermos o poder cibernético russo, necessitamos passar por uma retomada histórica. Observamos como Vladimir Putin chegou ao poder, onde ainda está, quase duas décadas depois. Durante os anos da administração de Putin, a Rússia, como o resto do mundo, vivenciou o desenvolvimento e a ascensão da internet e do ciberespaço, onde estes se tornaram um componente cotidiano da vida humana globalmente. Neste contexto, necessitamos refletir sobre a forma como a sociedade russa se desenvolveu e se acostumou à determinados autoritarismos que parecem estranhos à ideia de democracia existente no ocidente. Ainda, neste contexto, observamos o pensamento de Putin, em 1999, para os anos futuros, e pudemos contextualizar seu foco em expandir os poderes executivos e garantir a força do Estado com os acontecimentos posteriores, onde Moscou, através das forças federais de segurança, estatizou gigantes de mídia, petróleo e gás. Principalmente no caso da mídia, logo pudemos observar o tratamento do regime para com a questão da informação, tornando a imprensa um meio de propaganda estatal, evitando investimento privado na área ao máximo. O Kremlin havia visto na informação um agente importante de suas políticas logo no início da administração de Putin. Além disso, o fortalecimento das forças de segurança e o próprio desenvolvimento da sociedade criminosa acabaram sendo importantes vetores na evolução das capacidades cibernéticas de Moscou, quando observamos a grande incidência de atores obscuros em ações que envolvem interesses do Kremlin. A questão do controle sobre a sociedade e o fortalecimento das forças de segurança acaba desembocando no alto nível de controle sobre as atividades online, já que a informação era algo importante para o regime desde quando chegou ao poder.

Quando a internet começou a se tornar extremamente popular, e ainda pelas suas características, passou a ser um amplo campo de atuação de opositores políticos ao Kremlin. A utilização de mídias sociais passou a ser uma tendência generalizada na sociedade, e a rápida comunicação apresentavam um perigo à estabilidade do regime. Logo, as autoridades no Kremlin perceberam que necessitariam também se adentrar nesta questão, assim como nas telecomunicações e nos recursos energéticos. Rapidamente, com o apoio do Kremlin, a FSB passou a operar no ciberespaço, plantando agentes em várias comunidades de hackers para recrutar possíveis colaboradores, assim como aperfeiçoando suas habilidades próprias. Também, como observado em Smith, os criminosos cibernéticos eram hábeis na Rússia logo na virada do milênio pelo bom sistema educacional soviético, e sem muitos empregos na economia deficiente, o mercado das sombras do ciberespaço e do cibercrime acabava por ser o destino de muitos talentos na área. Assim sendo, a FSB tinha muito campo para explorar e, em essência, realizar uma operação de recrutamento. Apelando à nacionalismos em quase todas as questões polêmicas, O Kremlin viu os russos nacionalistas se tornarem uma poderosa arma cibernética a ser utilizada por agentes estatais, como bem observamos nos casos da Letônia, e até mesmo, possivelmente, nos EUA.

Logo, as autoridades em Moscou passaram a perceber a importância de operações online ao observarem os eventos da guerra da Chechênia. Quando importantes meios de comunicação dos chechenos eram abatidos, a moral e a força destes claramente diminuía. Os ataques cibernéticos de Moscou eram efetivos. Neste cenário, operadores da FSB passaram a induzir a ação de hackers nacionalistas nas comunidades que haviam se infiltrado anos antes. Quando a estátua soviética na Estônia foi removida, em 2007, não seria difícil encontrar algum russo desagradado com o fato. Os ataques cibernéticos que pararam a Estônia se provaram como uma forma eficiente de se mostrar presente e descontente. Afinal, o medo também gera influência. Após estes cenários, o Kremlin passou a enxergar as operações cibernéticas como importantes para desestabilizar o inimigo ou para preceder ataques convencionais, como aconteceu na Geórgia, em 2008. O que foi colocado na doutrina militar russa de 2010 é uma *de facto* aceitação dos fatos ocorridos nos anos anteriores e um anúncio de interesse e promessa de desenvolvimento na área. O Kremlin e seu braço militar logo perceberam que utilizar do espaço informacional do ciberespaço para atingir objetivos políticos sem o uso da força militar era uma grande arma, tanto internamente quanto externamente.

Quando os protestos em 2011 contra o governo ganharam força através de interações na internet, Moscou percebia mais ainda a importância de lidar com a informação doméstica

online. De fato, Putin passou a intensificar o controle sobre a rede, fato que pode ser notado quando o VK foi vendido à força para grupo conectado ao Kremlin. Logo, debilitar o discurso opositor político online e construir propaganda positiva passaram a ser um item importante para a política doméstica de Moscou, e nos eventos futuros, o Kremlin passaria a utilizar estas mesmas táticas para atingir objetivos de política externa. Com a evolução da participação do Estado no ciberespaço, que cresceu ainda mais com Medvedev, logo os russos aprendiam a operacionalizar efetivamente as táticas que observamos, como ataques DDoS ou a criação de *malware*.

Na guerra da Ucrânia, Moscou mostrou e ainda mostra que não se limita a derrubar sistemas de comunicação, ao proporcionar ações ofensivas contra redes elétricas em Kiev. Estas ações, nesta escala, não tem precedente. Neste cenário, o Kremlin parece ter superado as outras potências, ao menos na ousadia. Para as autoridades russas, aparentemente os limites das operações ofensivas no ciberespaço ainda não foram definidas. Em essência, a presença dos russos no ciberespaço se tornou muito grande devido ao sucesso deste tipo de operação e ao custo baixo que têm. Mas como bem observamos, Moscou não utiliza as mesmas armas em todos os casos, e apesar de se mostrar como um ator bem agressivo em seu exterior próximo, utiliza estratégias mais sutis para lidar com o ocidente. Em essência, as operações na Ucrânia mostram uma grande capacidade ofensiva da Rússia, que é impulsionada pelo controle que o Kremlin exerce sobre sua sociedade. Ainda, as operações na Geórgia e a doutrina militar mostram que os russos são proponentes na tal ciberguerra. O conflito cibernético é algo extremamente recente, e os limites para este ainda são desconhecidos a nós. Mas a Rússia parece ser uma firme proponente e parece ter de fato incorporado o *cyberwarfare* à suas políticas, até mesmo publicamente. É possível, através destas, identificar claramente que Moscou, até mesmo de maneira oficial, passou a tratar o ciberespaço como uma das principais áreas a serem exploradas, seja em questões de política externa ou de política interna.

Conclusivamente, observamos que o ciberespaço se tornou uma importante parte da convivência humana em sociedade. Os Estados, sendo os principais atores no sistema mundo, rapidamente passaram a agir para garantir a defesa e ampliação de seus interesses em uma nova plataforma que parecia estar cobrindo todos os fatores essenciais para a manutenção da sociedade. Neste cenário, ainda entendemos como a internet, por suas características únicas, se tornou um campo importante de divulgação de informação, e em determinadas ações, importante ponto de discussão política e debate público. Ali, Estados aprenderam que deveriam agir para se proteger e garantir a própria segurança nacional, em certos casos. Além disso, logo

perceberam que poderiam utilizar o ciberespaço para atingir determinados objetivos políticos, até mesmo externamente. Neste cenário, os Estados logo se encontrariam em um novo tipo de guerra, a cyberguerra, onde as capacidades cibernéticas seriam testadas e aplicadas, e conforme a tecnologia vai avançando, cada vez mais poderosas as armas cibernéticas vão se tornando.

Neste cenário, as grandes potências se tornaram os atores mais poderosos no ciberespaço. A Rússia de Vladimir Putin, por suas interessantes características internas e pelo formato como a sociedade se desenvolveu, além da flexibilidade e habilidade de gerenciamento da administração federal, passou a agir no ciberespaço tanto de maneira sutil, quanto de maneira agressiva, quando necessário. Com suas operações cibernéticas, passou a ser uma das principais proponentes no ciberespaço, rapidamente escalando suas operações para serem utilizadas em variadas situações, desde campanhas de desinformação em adversários estrangeiros e distantes até operações militares convencionais em seu exterior-próximo. Ainda, recentemente passou a intensificar suas operações e agir em vários *fronts*, onde busca ampliar suas vantagens estratégicas e desafogar as pressões que vêm sofrendo em outras áreas. Essencialmente, as políticas do Kremlin passaram a incorporar o *cyberwarfare* pois o custo das operações cibernéticas é baixo e os ganhos são altos, e além disso, o ciberespaço é uma importante ferramenta em constante transformação onde Moscou parece ter se tornado um dos agentes mais capazes, efetivamente sendo capaz de obter ganhos através de suas operações.

Para o futuro das relações cibernéticas internacionais, deveremos observar qual será a reação dos variados atores afetados por ações advindas do ciberespaço, incluindo o Kremlin. Enquanto que as campanhas de desinformação e as operações agressivas são efetivas, a probabilidade de algum tipo de regulamentação internacional sobre as ações pode ser enxergada no horizonte, mas algo concreto ainda está distante da realidade. Enquanto isto, e mesmo depois disto, cabe observarmos a capacidade ofensiva de atores cibernéticos para entendermos melhor o quão vulneráveis são estes sistemas interligados, e também esperar que as autoridades, organizações e empresas competentes sejam eficazes em garantir que a evolução do extremamente benéfico ciberespaço e sua incorporação na vida humana cotidiana não se transforme em uma rede de problemas crônicos sem solução.

REFERÊNCIAS

ABC NEWS. **Government Takes Russia's NTV.** 2000. Disponível em: <http://abcnews.go.com/International/story?id=81235> Acesso em 21/08/2017.

AMSTERDAM CITY COUNCIL. **Amsterdam's City Projects**. 2016. Disponível em: <https://amsterdamsmartcity.com/> Acesso em 12/10/2017.

BBC. **18 revelations from Wikileaks hacked Clinton emails.** 2016. Disponível em: <http://www.bbc.com/news/world-us-canada-37639370> Acesso em 15/10/2017.

BBC. **Alexander Livtinenko: Profile of murdered russian spy.** 2016. Disponível em: <http://www.bbc.com/news/uk-19647226> Acesso em 15/09/2017.

BBC. **Bears with keyboards: Russian hackers snoop on West.** 2016. Disponível em: <http://www.bbc.com/news/world-europe-37409456> Acesso em 15/10/2017.

BBC. **Heavy fighting rages near Donetsk**. 2015. Disponível em: <http://www.bbc.com/news/world-europe-32988499>. Acesso em 07/10/2017.

BBC. **How a cyber attack transformed Estonia**. 2017. Disponível em: <http://www.bbc.com/news/39655415>. Acesso em: 30/09/2017.

BBC. **Marine Le Pen: Who's funding France's far-right?** 2016. Disponível em: <http://www.bbc.com/news/world-europe-39478066> Acesso em 09/09/2017.

BBC. **Russia causing cyberspace "mayhem" says ex-GCHQ boss.** 2017. Disponível em: <http://www.bbc.com/news/technology-40557092> Acesso em 01/11/2017.

BBC. **Russia joins war in Syria.** 2015. Disponível em: <http://www.bbc.com/news/world-middle-east-34416519> Acesso em 22/10/2017.

BBC. **Russian election: biggest protests since fall of USSR.** 2011. Disponível em: <http://www.bbc.com/news/world-europe-16122524> Acesso em 15/09/2017.

BBC. **Twitter bans RT and Sputnik ads amid election interference fears.** 2017. Disponível em: <http://www.bbc.com/news/world-us-canada-41766991> Acesso em 02/11/2017.

BRYANT, Rebecca. **What Kind Of Space Is Cyberspace?** Minerva 5. P. 138-155. Londres. 2001.

BUSINESS INSIDER. **China bans Uber**. 2015. Disponível em: <http://www.businessinsider.com/uber-china-ban-2015-1> Acesso em 13/10/2017.

BUSINESS INSIDER. **Explanation to polarization on US politics.** 2017. Disponível em: <http://www.businessinsider.com/sociology-explains-polarization-politics-2017-3> Acesso em 21/10/2017.

BUSINESS INSIDER**. US and European Energy Companies hit by cyberweapon**. 2014. Disponível em: <http://www.businessinsider.com/energetic-bear-virus-and-energy-companies-2014-7> Acesso em 20/10/2017

CDT. **The world of Official Espionage.** 2013. Disponível em: <http://chinadigitaltimes.net/2013/02/wiretapping-wars-the-world-of-official-espionage/> Acesso em 10/09/2017.

CNBC. **Trump to CNN Reporter: You are fake news**. 2017. Disponível em: <https://www.cnbc.com/video/2017/01/11/trump-to-cnn-reporter-you-are-fake-news.html> Acesso em 01/11/2017.

CNET. **Georgia accuses Russia of coordinated cyberattack.** 2008. Disponível em: <https://www.cnet.com/news/georgia-accuses-russia-of-coordinated-cyberattack/> Acesso em 20/10/2017

C-NET. **Stuxnet delivered on drive.** 2012. Disponível em: <https://www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/> Acesso em 10/10/2017.

CNN. **Medvedev wants Russia to go hi-tech.** 2009. Disponível em: <http://edition.cnn.com/2009/WORLD/europe/11/12/russia.medvedev.speech/> Acesso em 06/07/2017

CNN. **Russia the third largest military spender.** 2017. Disponível em: <http://money.cnn.com/2017/04/24/news/russia-military-spending/index.html> Acesso em 29/10/2017.

CNN. **Vladimir's Vacations**. 2017. Disponível em: <http://edition.cnn.com/2017/08/05/politics/putin-vacation-siberia/index.html> Acesso em 10/08/2017.

CONNEL, M; VOGLER, S. **Russia's approach to cyberwarfare**. 2017. Disponível em: <https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf>. Acesso em: 30/09/2017.

DAILYMAIL. GEORGIA. **"Overrun" by Russian troops**. 2008. Disponível em: <http://www.dailymail.co.uk/news/article-1043236/Georgia-overrun-Russian-troops-scale-ground-invasion-begins.html> Acesso em: 30/09/2017.

DAWISHA, Karen. **Putin's Kleptocracy**. New York. 2016.

DER SPIEGEL. **Iran's nuclear program hit by computer virus.** Disponível em: <http://www.spiegel.de/netzwelt/gadgets/irans-atomprogramm-ahmadinedschad-raeumt-virus-attacke-ein-a-731881.html> Acesso em 21/09/2017.

DER SPIEGEL. **Secret Links between Germany and the NSA.** 2013. Disponível em: <http://www.spiegel.de/international/world/german-intelligence-worked-closely-with-nsa-on-data-surveillance-a-912355.html> Acesso em: 10/10/2017

DESAI, Padma. **Russian retrospectives on reforms from Yeltsin to Putin.** 2005. Disponível em: <http://faculty.nps.edu/relooney/00_New_13.pdf> Acesso em 10/10/2017.

DFR LAB. **The Kremlin's Audience in France.** 2017. Disponível em: <https://medium.com/dfrlab/the-kremlins-audience-in-france-884a80515f8b> Acesso em 15/10/2017.

E-ISAC. **Analysis of the cyber attack on the Ukrainian power grid**. Disponível em: <https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf> Acesso em 05/10/2017

EL PAÍS. **O problema do cibercrime no Brasil. 2015.** Disponível em: <https://brasil.elpais.com/brasil/2015/10/23/opinion/1445558339_082466.html> Acesso em 10/10/2017

FGV. DAPP. **Robôs, redes sociais e política no Brasil**. 2017. Disponível em: <http://dapp.fgv.br/wp-content/uploads/2017/08/Robos-redes-sociais-politica-fgv-dapp.pdf>

FINANCIAL TIMES. **Stuxnet causes worldwide alarm.** 2010. Disponível em: <https://www.ft.com/content/cbf707d2-c737-11df-aeb1-00144feab49a?mhq5j=e6> Acesso em 20/10/2017.

FOKIN, Alexander**. Internet Trolling as a tool of hybrid warfare: The case of Latvia**. NATO Strategic Communication Centre of Excellence. 2016.

FOLHA DE S. PAULO. **Putin se reúne com Le Pen.** 2017. Disponível em: <http://www1.folha.uol.com.br/mundo/2017/03/1869375-em-moscou-putin-se-reune-com-a-ultradireitista-francesa-marine-le-pen.shtml> Acesso em 09/10/2017.

FOLHA DE S. PAULO. **RT: Noticias ou Propaganda?** 2017. Disponível em: <http://www1.folha.uol.com.br/mundo/2017/03/1865017-emissora-russa-rt-e-agencias-de-noticias-ou-propaganda-do-kremlin.shtml> Acesso em 09/09/2017.

FORBES. **End of the Silk Road.** 2013. Disponível em: <https://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/> Acesso em 10/10/2017.

FORBES. **How Google Ads works.** 2014. Disponível em: <https://www.forbes.com/sites/quora/2014/08/15/how-exactly-does-google-adwords-work> Acesso em 07/10/2017.

FORBES. **One year after Russia annexed Crimea, locals prefer Moscow to Kiev**. 2015. Disponível em: <https://www.forbes.com/sites/kenrapoza/2015/03/20/one-year-after-russia-annexed-crimea-locals-prefer-moscow-to-kiev/> Acesso em 21/10/2017.

FORBES: **Inside Ukraine's power outage.** 2016. Disponível em: <https://www.forbes.com/sites/thomasbrewster/2016/01/04/ukraine-power-out-cyber-attack/#27f158416fa8> Acesso em 10/10/2017

FOREIGN AFFAIRS. **Putin and the Oligarchs.** 2004. Disponível em: <https://www.foreignaffairs.com/articles/russia-fsu/2004-11-01/putin-and-oligarchs> Acesso em 09/09/2017.

FT. **Ukraine's security chief accuses Russia of waging hybrid war.** Disponível em: <https://www.ft.com/content/789b7110-e67b-11e3-9a20-00144feabdc0> Acesso em 27/10/2017.

G1. **Ataque hacker ao Planalto.** 2011. Disponível em: <http://g1.globo.com/tecnologia/noticia/2011/06/ataque-hacker-foi-o-maior-ja-sofrido-por-sites-do-governo-na-internet.html> Acesso em 03/10/2017.

GIBNEY, Alex. **Zero Days**. 2016. Londres.

GITHUB. **GitHub under large scale DDoS attack.** 2015. Disponível em: <https://github.com/blog/1981-large-scale-ddos-attack-on-github-com> Acesso em 21/09/2017.

GOVERNO FEDERAL RUSSO. **Doutrina militar russa.** 2010. Moscou. Disponível em: <http://carnegieendowment.org/files/2010russia_military_doctrine.pdf>. Acesso em: 30/09/2017.

HARVARD. **Empirical Analysis of Internet Filtering in China.** 2003. Disponível em: <https://cyber.harvard.edu/filtering/china/> Acesso em 07/10/2017.

HUFFINGTON POST. **Social media and the 2016 presidential election.** 2017. Disponível em: <https://www.huffingtonpost.com/r-kay-green/the-game-changer-social-m_b_8568432.html> Acesso em 16/10/2017.

ICG. **Key features of Iran's Nuclear Program**. 2015. Disponível em: <http://blog.crisisgroup.org/worldwide/2015/09/10/key-features-of-irans-nuclear-program/> Acesso em 12/09/2017

INTERNET LIVE STATS. **Internet Stats.** Disponível em: <http://www.internetlivestats.com/internet-users/> Acesso em 10/10/2017

LIBICKI, Martin. **Conquest in Cyberspace: National Security and Information Warfare.** Cambridge University Press, 2007. Cambridge.

LIPMAN, Masha. **"Managed Democracy" in Russia.** 2001.

LUKIN, Alexander. **Electoral Democracy or Electoral Clanism?** 2016. Disponível em: <http://www2.gwu.edu/~ieresgwu/assets/docs/demokratizatsiya%20archive/07-01_lukin.pdf>

MANNESS, Ryan. **Cyber policy as a source of power. Russia in Cyberspace**. London. 2015.

MINISTÉRIO DAS RELAÇÕES EXTERIORES DA GEÓRGIA. **Cyber attacks disable georgian websites.** 2008. Disponível em: <http://georgiamfa.blogspot.com.br/2008/08/cyber-attacks-disable-georgian-websites.html>. Acesso em: 30/09/2017.

MIT. **Six lessons from Amsterdam's Smart City Initiative**. 2016. Disponível em: <http://sloanreview.mit.edu/article/six-lessons-from-amsterdams-smart-city-initiative/> Acesso em 20/10/2017

NANCE, Malcolm. **The Plot to Hack America: How Putin's cyberspies and Wikileaks tried to steal the 2016 election.** Skyhorse Publishing. 216 p. New York. 2016.

NETRESEC. **China's Man-on-the-Side attack on GitHub.** 2015. Disponível em: <http://www.netresec.com/?page=Blog&month=2015-03&post=China%27s-Man-on-the-Side-Attack-on-GitHub> Acesso em 01/10/2017.

NEW YORK TIMES. **Mueller seeks White House documents related to Trump**. 2017. Disponível em: <https://www.nytimes.com/2017/09/20/us/politics/mueller-trump-russia.html> Acesso em 02/11/2017.

NEW YORK TIMES**: Israeli test on worm called crucial in Iran.** Disponível em: <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?mcubz=3> Acesso em 20/10/2017

NEWTON, Matthew. **Russia Media Profile: Digital patriotism and Nationalist Agenda**. 2017. Disponível em: <https://jsis.washington.edu/news/russia-media-profile-digital-patriotism-nationalist-agenda/> Acesso em 15/10/2017

NY TIMES. **Crimea in dark after power lines are blown up**. 2015. Disponível em: <https://www.nytimes.com/2015/11/23/world/europe/power-lines-to-crimea-are-blown-up-cutting-off-electricity.html> Acesso em 20/10/2017

NY TIMES. FBI. **The fake americans.** 2017. Disponível em: <https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html> Acesso em 10/10/2017

NY TIMES. **Russian security agencies raid media empire's offices.** 2000. Disponível em: <http://www.nytimes.com/2000/05/12/world/russian-security-agencies-raid-media-empire-s-offices.html> Acesso em 10/09/2017.

NYE, Joseph S. **Cyber Power.** Harvard Kennedy School. Belfer Center. 2010. Disponível em: <https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf>

PARKER, Emily. **Putin's Cyberphobia.** Londres. 2014.

POLITICO. **All of Trump's Russia Ties.** 2017. Disponível em: <https://www.politico.com/magazine/story/2017/03/connections-trump-putin-russia-ties-chart-flynn-page-manafort-sessions-214868> Acesso em 02/11/2017.

POMERANTSEV, Peter. **Russia: A post-modern dictatorship?** 2013. Londres.

PRESSTV. **Wikileaks will take down America, says CIA director**. 2017. Disponível em: <http://www.presstv.com/Detail/2017/07/21/529155/WikiLeaks-will-take-down-America-CIA-director> Acesso em 08/10/2017.

PUTIN, Vladimir. **Russia at the turn of the millennium.** 1999. Disponível em: <http://pages.uoregon.edu/kimball/Putin.htm> Acesso em 09/10/2017.

REUTERS. **Chinese company helps Iran spy on its citizens**. 2012. Disponível em: <http://www.reuters.com/article/us-iran-telecoms/special-report-chinese-firm-helps-iran-spy-on-citizens-idUSBRE82L0B820120322> Acesso em 10/10/2017.

REUTERS. **Russia-Trump campaign collusion an open issue.** 2017. Disponível em: <https://www.reuters.com/article/us-usa-trump-russia-senate-collusion/russia-trump-campaign-collusion-an-open-issue-u-s-senate-panel-chiefs-idUSKBN1C92G3> Acesso em 23/10/2017.

REUTERS. **Two-thirds of American adults get news from social media**. 2017. Disponível em: <https://www.reuters.com/article/us-usa-internet-socialmedia/two-thirds-of-american-adults-get-news-from-social-media-survey-idUSKCN1BJ2A8> Acesso em 19/10/2017.

REUTERS. **Ukraine hit by 6,500 hack attacks, sees Russian cyberwar.** Disponível em: <https://www.reuters.com/article/us-ukraine-crisis-cyber/ukraine-hit-by-6500-hack-attacks-sees-russian-cyberwar-idUSKBN14I1QC> Acesso em 28/10/2017

REUTERS. **Ukraine points finger at Russian security services in recent cyber attack.** 2014. Disponível em: <https://www.reuters.com/article/us-cyber-attack-ukraine-idUSKBN19M39P> Acesso em: 15/10/2017

REUTERS. **Ukraine to probe suspected Russian cyber attack on grid.** 2016. Disponível em: <http://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UE0ZZ20151231> Acesso em 21/10/2017

REVERON, Derek S. **Cyberspace and National Security**: Threats, opportunities, and Power in a virtual world. Georgetown: Georgetown University Press, 2012. 272 p.

REVISTA VEJA. **Ucrânia diz que 30.000 soldados russos ocupam a Crimeia**. 2016. Disponível em: <http://veja.abril.com.br/mundo/ucrania-diz-que-30-000-soldados-russos-ocupam-a-crimeia/> Acesso em: 30/09/2017.

RFI, LE MONDE. **French government accused of widespread spying**. 2013. Disponível em: <http://en.rfi.fr/france/20130705-french-government-accused-widespread-spying-its-own-citizens> Acesso em 10/10/2017

RT. **Ed Schultz comments on investigations.** 2017. Disponível em: <https://www.rt.com/usa/408527-ed-schultz-russia-investigation-alleged-meddling/> Acesso em 21/10/2017.

RT. **Role of Hillary Clinton in Lybia war exposed.** 2016. Disponível em: <https://www.rt.com/usa/334400-hillary-clinton-libya-role/> Acesso em 02/11/2017.

RT. **Russia will respond to NATO expansion – Putin.** 2017. Disponível em: <https://www.rt.com/news/392166-putin-stone-nato-expansion/> Acesso em 29/10/2017.

SAKWA, Richard. **Putin: Russia's Choice**. Londres. Routledge, 2004.

SECUREWORKS. **Advanced Persistent Threats**. Disponível em: <https://www.secureworks.com/blog/advanced-persistent-threats-apt-a> Acesso em 10/10/2017

SILVA, Narjara Bárbara Xavier; **Engenharia social nas redes sociais online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação.** Revista Ibero-Americana de Ciência da Informação, [S.l.], v. 6, n. 2, mar. 2014. ISSN 1983-5213. Disponível em: <http://periodicos.unb.br/index.php/RICI/article/view/9222>. Acesso em: 12/10/2017.

SMITH, David. **How Russia Harnesses Cyberwarfare**. 2012. Disponível em: <http://www.afpc.org/files/august2012.pdf>. Acesso em: 30/09/2017.

SOLDATOV, Andrei; BOROGAN, Irina. **The New Nobility:** The restoration of Russia's security state and the enduring legacy of the KGB. Nova Iorque: PublicAffairs, 2011. 318 p.

STRATFOR. **The rise and fall of Russian oligarchs.** 2009. Disponível em: <https://wikileaks.org/gifiles/attach/144/144365_RussianoligarchPDF.pdf>

TECHCRUNCH. **Durov out of VK for good.** 2014. Disponível em: <https://techcrunch.com/2014/04/22/durov-out-for-good-from-vk-com-plans-a-mobile-social-network-outside-russia/> Acesso em 15/09/2017

TECHINASIA. **China now has 731 million internet users**. 2017. Disponível em: <https://www.techinasia.com/china-731-million-internet-users-end-2016> Acesso em 15/09/2017.

TECHTARGET. **Zombies**. Disponível em: <http://searchmidmarketsecurity.techtarget.com/definition/zombie> Acesso em 01/10/2017

THE ECONOMIST. **The birth of a Tsar.** 2017. Disponível em: <https://www.economist.com/news/leaders/21730645-world-marks-centenary-october-revolution-russia-once-again-under-rule> Acesso em 02/11/2017.

THE GUARDIAN. **DNC email leak: Russian hackers Cozy Bear and Fancy Bear behind breach.** 2016. Disponível em: <https://www.theguardian.com/technology/2016/jul/26/dnc-email-leak-russian-hack-guccifer-2> Acesso em 21/10/2017.

THE GUARDIAN. **Edward Snowden's plane lands in Moscow**. 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/23/edward-snowden-arrives-moscow> Acesso em 20/10/2017.

THE GUARDIAN. **FSB: Vladimir Putin's immensely powerful modern-day KGB**. 2013. Disponível em: <https://www.theguardian.com/world/2013/oct/06/fsb-putins-modern-day-kgb> Acesso em 06/09/2017.

THE GUARDIAN. **Iran accuses Siemens of helping US and Israel with Stuxnet.** 2011. Disponível em: <https://www.theguardian.com/world/2011/apr/17/iran-siemens-stuxnet-cyber-attack> Acesso em 15/10/2017

THE GUARDIAN. **Iran nuclear scientist killed in bomb attack**. Disponível em: <https://www.theguardian.com/world/2010/nov/29/iran-nuclear-scientist-bomb-attack> Acesso em 20/10/2017

THE GUARDIAN. NATO. **Moves to bolster eastern European defences against Russia**. 2014. Disponível em: <https://www.theguardian.com/world/2014/apr/01/nato-eastern-europe-defences-russia-putin-crimea>. Acesso em: 30/09/2017.

THE GUARDIAN. **Nemtsov family dismisses verdict.** 2017. Disponível em: <https://www.theguardian.com/world/2017/jun/29/gunman-found-guilty-murdering-russian-opposition-leader-boris-nemtsov> Acesso em 08/08/2017.

THE GUARDIAN. **NSA mass surveillance ruled illegal by Federal Court.** 2013. Disponível em: <https://www.theguardian.com/us-news/2015/may/07/nsa-phone-records-program-illegal-court> Acesso em 10/10/2017

THE GUARDIAN. **Obama backs Macron in last-minute intervention in French election.** 2017. Disponível em: <https://www.theguardian.com/world/2017/may/04/barack-obama-backs-macron-in-last-minute-election-intervention> Acesso em 21/10/2017.

THE GUARDIAN. **Obama promises retaliation against Russian hacking.** 2016. Disponível em: <https://www.theguardian.com/us-news/2016/dec/16/obama-retaliation-russia-hacking-us-election> Acesso em 15/10/2017.

THE GUARDIAN. **Oligarch flees Russia for new life in Britain**. 2009. Disponível em: <https://www.theguardian.com/world/2009/jan/27/russia-kremlin-oligarchs> Acesso em 07/10/2017.

THE GUARDIAN. **Protest by Kremlin as police quell riots in Estonia**. 2007. Disponível em: <https://www.theguardian.com/world/2007/apr/29/russia.lukeharding>. Acesso em: 30/09/2017.

THE GUARDIAN. **Snowden leaves Hong Kong**. 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/23/edward-snowden-leaves-hong-kong-moscow> Acesso em 20/10/2017.

THE GUARDIAN. **The NSA Files.** 2013. Disponível em: <https://www.theguardian.com/us-news/the-nsa-files> Acesso em 20/10/2017.

THE GUARDIAN. **Top democrat e-mails hacked.** Disponível em: <https://www.theguardian.com/us-news/2016/dec/14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds> Acesso em 10/10/2017.

THE INDEPENDENT. **China planning it's own wikipedia version**. 2017. Disponível em: <http://www.independent.co.uk/news/world/asia/china-wikipedia-chinese-version-government-no-public-authors-contributions-communist-party-line-a7717861.html> Acesso em 25/10/2017

THE INDEPENDENT. **Trump's approval rating falling.** 2017. Disponível em: <http://www.independent.co.uk/news/world/americas/us-politics/trump-approval-rating-polls-popularity-latest-fall-states-a7995201.html> Acesso em 27/10/2017.

THE INDEPENDENT. **Vladimir Putin hints at 'patriotic' private hackers interference in US election.** 2017. Disponível em:< http://www.independent.co.uk/news/world/americas/us-politics/vladimir-putin-russian-hackers-patriotic-private-us-election-2016-donald-trump-win-dnc-hillary-a7767436.html>. Acesso em: 30/09/2017.

THE TELEGRAPH. **How Stuxnet works**. 2011. Disponível em: <http://www.telegraph.co.uk/technology/8274488/How-Stuxnet-works-what-the-forensic-evidence-reveals.html> Acesso em: 18/09/2017

THE WASHINGTON POST. **Snowden comes forward.** 2013. Disponível em: <https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html?utm_term=.700bec1eb827> Acesso em: 20/10/2017.

TIME MAGAZINE. **Donald Trump attacks Clinton on her marriage.** 2016. Disponível em: <http://time.com/4515676/donald-trump-hillary-clinton-bill-clinton-marriage/> Acesso em 15/10/2017.

TIME MAGAZINE. **Operation Titan Rain.** 2005. Disponível em: <https://courses.cs.washington.edu/courses/csep590/05au/readings/titan.rain.htm> Acesso em 05/10/2017.

U.S GOVERNMENT. **Public Law no. 110-140 (19/12/2007).** Disponível em: <https://www.congress.gov/bill/110th-congress/house-bill/6/text> Acesso em 10/10/2017

US GOVERNMENT. **NIST. Guidelines for Smart Grid Cybersecurity**. 2014. Disponível em: <http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf> Acesso em 10/10/2017

US GOVERNMENT. **What is a smart grid?** 2016. Disponível em: <https://www.smartgrid.gov/the_smart_grid/smart_grid.html> Acesso em 15/06/2017

VK. **User catalog.** 2017. Disponível em: <https://vk.com/catalog.php> Acesso em 10/10/2017

WASHINGTON POST. **How Trump won the presidency with razor-thin margins in swing states.** 2016. Disponível em: <https://www.washingtonpost.com/graphics/politics/2016-election/swing-state-margins/> Acesso em 21/10/2017.

WASHINGTON POST. **The Trump campaign's attempted collusion**. 2017. Disponível em: <https://www.washingtonpost.com/opinions/the-trump-campaigns-attempted-collusion/2017/07/10/7841c090-65b0-11e7-8eb5-cbccc2e7bfbf_story.html?utm_term=.2c084ac56c24> Acesso em 21/10/2017.

WELIVESECURITY. **Blackenergy strikes again.** Disponível em: <https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/> Acesso em 25/10/2017.

WIRED. **Hackers take down the most wired country in Europe.** 2007. Disponível em: <https://www.wired.com/2007/08/ff-estonia/>. Acesso em: 30/09/2017.

WIRED. **Russia's Fancy Bear hackers.** Disponível em: <https://www.wired.com/story/fancy-bear-hotel-hack/> Acesso em 21/10/2017.

WORTZEL, Larry. **Cyberespionage and the theft of US intellectual property**. 2013. Disponível em: <http://docs.house.gov/meetings/IF/IF02/20130709/101104/HHRG-113-IF02-Wstate-WortzelL-20130709-U1.pdf>

WSJ. **Virus infects Chevron Network.** 2012. Disponível em: <https://www.wsj.com/articles/SB10001424127887324894104578107223667421796> Acesso em 20/10/2017

ZETTER, Kim. **Countdown to Zero Day: Stuxnet and the Launch of the World's first digital weapon**. Broadway Books, 2015.