UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO SOCIOECONÔMICO
DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS
CURSO DE GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

Matheus Eduardo Neuenfeld

Estratégia Nacional e Poder Cibernético: o ressurgimento da Rússia no cenário internacional

Florianópolis,
2021

Matheus Eduardo Neuenfeld

Estratégia Nacional e Poder Cibernético: o ressurgimento da Rússia no cenário internacional

Trabalho de Conclusão de Curso de Graduação em Relações Internacionais do Centro Socioeconômico da Universidade Federal de Santa Catarina, como requisito obrigatório para a obtenção do título de Bacharel em Relações Internacionais.
Orientadora: Prof.(a) Danielle Jacon Ayres Pinto, Dra.

Florianópolis,

2021

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

Neuenfeld, Matheus Eduardo
Estratégia nacional e poder cibernético : o ressurgimento da Rússia no cenário internacional / Matheus Eduardo Neuenfeld ; orientadora, Danielle Jacon Ayres Pinto, 2021.
137 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro Sócio Econômico, Graduação em Relações Internacionais, Florianópolis, 2021.

Inclui referências.

1. Relações Internacionais. 2. Segurança e defesa. 3. Poder cibernético. 4. Guerra híbrida. I. Ayres Pinto, Danielle Jacon . II. Universidade Federal de Santa Catarina. Graduação em Relações Internacionais. III. Título.

Matheus Eduardo Neuenfeld

Estratégia Nacional e Poder Cibernético:
o ressurgimento da Rússia no cenário internacional

Florianópolis, 07 de maio de 2021

O presente Trabalho de Conclusão de Curso foi avaliado e aprovado pela banca examinadora composta pelos seguintes membros:

Profª. Drª. Danielle Jacon Ayres Pinto
Universidade Federal de Santa Catarina

Profª. Drª. Graciela de Conti Pagliari
Universidade Federal de Santa Catarina

Profª. Drª. Larlecianne Piccolli
InterAgency Institute

Certifico que esta é a **versão original e final** do Trabalho de Conclusão de Curso que foi julgado adequado para obtenção do título de Bacharel em Relações Internacionais por mim e pelos demais membros da banca examinadora.

Documento assinado digitalmente
Danielle Jacon Ayres Pinto
Data: 14/05/2021 12:08:08-0300
CPF: 291.367.488-70
Verifique as assinaturas em https://v.ufsc.br

_____

Profª. Drª Danielle Jacon Ayres Pinto
Orientadora

Florianópolis, 2021

AGRADECIMENTOS

Em primeiro lugar eu agradeço à minha família, especialmente à minha mãe, Evanir, minha irmã, Débora e meu irmão, Rodrigo. Muito obrigado por tudo o que fizeram por mim até hoje, todo o apoio, conselhos e conversas. Eu sou privilegiado por toda a estrutura material e emocional que eu tive para chegar até aqui, e isso eu devo a vocês.

Aos meus amigos de vida e de UFSC, por todos os momentos de apoio, conversas e de descontração. Vocês foram essenciais para a conclusão da minha jornada na UFSC e a concretização desse trabalho.

Aos professores que eu tive ao longo da minha jornada acadêmica na UFSC, bem como os que me acompanharam durante a minha educação básica. O ensino é essencial para que o país cresça e se desenvolva de forma sustentável, mas um bom ensino só se faz com bons professores, pessoas que dedicam suas vidas à essa profissão elementar. Portanto, parabéns a todos vocês e muito obrigado por tudo que fizeram e ainda fazem pela educação brasileira.

Presto igualmente o agradecimento à minha orientadora, professora Danielle, uma pessoa de um saber imenso e que me auxiliou em todas as fases desse trabalho.

Por fim, agradeço ao sistema público de ensino brasileiro e a UFSC, que mesmo diante de tantas dificuldades ainda resistem e servem como a esperança de muitos cidadãos brasileiros que buscam um futuro melhor para si e para as suas famílias.

"*Not everyone likes the stable, gradual rise of our country* […] *There are some who are using the democratic ideology to interfere in our internal affairs*."

(Vladimir Putin)

RESUMO

Este trabalho tem como objetivo analisar de que modo a Rússia emprega os seus recursos cibernéticos como instrumentos de defesa nacional. A parte inicial do trabalho apresenta um arcabouço que discute a leitura do poder cibernético a partir da perspectiva das teorias neorealista e construtivista das relações internacionais, a securitização e instrumentalização do ciberespaço e a relação entre a tecnologia e a guerra. A análise da política estratégica da Rússia no século XXI, abordando-se os aspectos de política interna, política externa e política de segurança e defesa, demonstra o aumento da assertividade e da agressividade das ações russas. O comportamento dos EUA e da OTAN mostram-se como desestabilizadores do sistema internacional e uma ameaça à segurança e aos interesses nacionais russos. O ciberespaço é enxergado pela Rússia a partir de uma interpretação dual que considera tanto aspectos técnico-computacionais como também informacional-psicológicos. A informação é considerada como um ativo estratégico pelo país, fonte de ameaças e de oportunidades, principalmente em termos de uso ofensivo como um instrumento assimétrico e dissuasório. As capacidades cibernéticas russas estão principalmente ligadas com as agências de segurança e inteligência do país, mas também guardam relação com *proxies*. O emprego de recursos cibernéticos está sustentado pela doutrina militar-estratégica russa, que apresenta os conceitos de meios cinéticos e não-cinéticos e os seus usos ofensivos para garantir a segurança nacional russa. No nível operacional a execução do poder cibernético russo se desenvolve por meio do que se conhece como Guerra Híbrida. Os casos da Estônia, Geórgia, Ucrânia e EUA, mostram que o emprego de recursos cibernéticos pela Rússia obedece à uma lógica estratégica que busca evitar o confronto direto com as potências internacionais, adaptando-se a abordagem com meios cinéticos (operações militares) e meios não cinéticos (operações cibernéticas e de informação) conforme o cenário imposto.

Palavras-chave: Rússia, Poder cibernético, Ciberespaço, Operações cibernéticas, Operações de informação, Guerra Híbrida.

ABSTRACT

This paper aims to analyze how Russia uses its cyber resources as instruments of national defense. The initial part of the work presents a framework that discusses the reading of cyber power from the perspective of the neorealistic and constructivist theories of international relations, the securitization and instrumentalization of cyberspace and the relationship between technology and war. The analysis of Russia's strategic policy in the 21st century, addressing aspects of domestic policy, foreign policy and security and defense policy, demonstrates the increased assertiveness and aggressiveness of Russian actions. The behavior of the USA and NATO is seen as destabilizing the international system and a threat to Russian security and national interests. Cyberspace is seen by Russia from a dual interpretation that considers both technical-computational as well as informational-psychological aspects. Information is considered a strategic asset by the country, a source of threats and opportunities, mainly in terms of offensive use as an asymmetric and deterrent tool. Russian cyber capabilities are mainly linked to the country's security and intelligence agencies, but they are also related to proxies. The use of cyber resources is supported by Russian military-strategic doctrine, which presents the concepts of kinetic and non-kinetic means and their offensive uses to guarantee Russian national security. At the operational level, the execution of Russian cyber power takes place through what is known as the Hybrid Warfare. The cases of Estonia, Georgia, Ukraine and the USA, show that the use of cyber resources by Russia obeys a strategic logic that seeks to avoid direct confrontation with international powers, adapting the approach with kinetic means (military operations) and not kinetic means (cyber and information operations) according to the imposed scenario.

Keywords: Russia, Cyber Power, Cyberspace, Cyber Operations, Information Operations, Hybrid Warfare.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

API Agência de Pesquisas na Internet

BM Banco Mundial

CEI Comunidade dos Estados Independentes

CIA *Central Intelligence Agency*

CyberOps Operações Cibernéticas

CNO *Computer Network Operations*

CPE Conceito de Política Externa

DCCC *Democratic Congressional Campaign Committee*

DDoS *Distributed Denial-of-Service*

DoD *Department of Defense*

DM Doutrina Militar

DNC *Democratic National Committee*

DSI Doutrina de Segurança da Informação

ESN Estratégia de Segurança Nacional

EUA Estados Unidos da América

FAPSI *Federal'noye Agentstvo Svyazi i Pravitel'stvennoy Informatsii* (Agência Federal de Comunicações e Informações Governamentais)

FSB *Federalnaya Sluzhba Bezopasnosti* (Serviço de Segurança Federal)

FSO *Federalnaya Sluzhba Okhrany* (Serviço de Proteção Federal)

GH Guerra Híbrida

GRU *Glavnoye Razvedyvatel'noye Upravleniye* (Diretório Central de Inteligência)

INF *Intermediate-Range Nuclear Forces Treaty*

InfoOps Operações de Informação

ISP *Internet Service Provider*

KGB *Komitet Gosudarstvennoy Bezopasnosti* (Comitê de Segurança do Estado)

OACI Organização da Aviação Civil Internacional

OCX Organização para a Cooperação de Xangai

OMI Organização Marítima Internacional

ONU Organização das Nações Unidas

OTAN Organização do Tratado do Atlântico Norte

OTSC Organização do Tratado de Segurança Coletiva

PIB Produto Interno Bruto

PsyOps Operações Psicológicas

RBN *Russian Business Network*

SCADA *Supervisory Control and Data Acquisition*

START *Strategic Arms Reduction Treaty*

SBU *Sluzhba Bezpeky Ukrayiny* (Serviço de Segurança da Ucrânia)

SVR *Sluzhba Vneshney Razvedki* (Serviço de Inteligência Externa)

UE União Europeia

URSS União das Repúblicas Socialistas Soviéticas

SUMÁRIO

1 INTRODUÇÃO

As características próprias do ciberespaço fazem desse um ambiente relevante para a política internacional. Isso porque o meio cibernético promoveu significativas transformações na forma como a informação é criada e transmitida, alterando as dinâmicas entre Estados e organizações não-estatais, o que permitiu uma difusão do poder entre esses atores do sistema internacional. Fatores como a anonimidade, o baixo custo de acesso e a assimetria de vulnerabilidades fizeram com que mesmo atores que antes não possuíam capacidades materiais de atuação no cenário internacional, passassem agora a empreender *hard* e *soft power* por meio da cibernética (NYE, 2010).

Assim, os Estados passam a observar um ambiente composto por cada vez mais atores, se tornando mais complexo e desafiador o controle e compreensão do fluxo de um elemento primordial: a informação (NYE, 2010). O interesse expresso dos Estados sobre as repercussões advindas do domínio externo, seja estatal ou não, sobre as informações que compõem e suportam as mais diversas áreas da sociedade e das instituições de governo, torna a defesa cibernética fundamental para manutenção da segurança nacional, bem como, para a projeção de poder.

Nesse contexto, a Rússia é um país de destaque no que se refere ao emprego ofensivo de meios cibernéticos. O Estado russo alegadamente esteve envolvido em diversos acontecimentos relevantes da política internacional nos quais foram identificadas atividades cibernéticas contra países em contextos específicos (BLANK, 2017). Além disso, a ocorrência de ações cibernéticas em episódios em que foram também verificadas operações militares, enquanto em outras ocasiões observou-se somente a aplicação de instrumentos não-cinéticos, são os fatores que justificam a escolha da Rússia como elemento de análise desse trabalho.

Como mostram Connell e Vogler (2017), o governo russo entende que está sendo pressionado por forças internas e externas que pretendem desafiar a segurança nacional do país por meio da esfera da informação. Assim sendo, o fluxo de informação que ocorre através da internet é enxergado como uma ameaça e, ao mesmo tempo, como uma oportunidade pelo Estado russo.

Nota-se que os recursos de poder cibernético já representam significativa presença no conjunto de forças ofensivas russas, conjuntamente como o espectro militar convencional. Os fatos ocorridos na Geórgia (2008) e Ucrânia (2014) demonstram como as duas vertentes das forças ofensivas da Rússia operam conjuntamente para a concretização de objetivos militares e geopolíticos, estratégia conhecida como guerra híbrida (CONNEL; VOGLER, 2017).

Da perspectiva dos teóricos estrategistas e militares russos, o ponto essencial da atuação no ciberespaço é o estabelecimento de uma superioridade informacional, como forma de exercer poder. É em função disso que a matéria é versada pelos documentos oficiais do país como "Espaço da Informação", aludindo ao fato de que o controle da criação e fluxo da informação gera a capacidade de confundir e descapacitar adversários, limitando a propensão a resistência e aumentando a inclinação pela dissuasão (JAITNER, 2015).

As consequências da estratégia nacional de defesa russa por meio das ofensivas no campo cibernético, e além dele, já são notadas e despertam alertas em países ocidentais, uma vez que as ameaças às instituições de Estado e ao funcionamento ótimo das sociedades nacionais são cada vez mais palpáveis, dado o nível de integração de sistemas informatizados como resultado das novas soluções de TIC (LEWIS, 2015).

Nessa lógica, a questão que cerca a estratégia russa de uso conjunto de recursos cibernéticos com as forças militares convencionais para exercer poder no cenário internacional levanta indagações sobre como essa política afeta os países atingidos e se reproduz na proeminência de influência do Estado russo, engendrando simultaneamente uma potencial nova corrida armamentista em busca de recursos ofensivos cibernéticos (JAITNER, 2015; POLYAKOVA; BOYER, 2018).

Dado esse contexto, o tema central deste trabalho é o emprego de recursos de poder cibernético como instrumentos de defesa nacional. Em particular, este estudo versa sobre a utilização desses instrumentos no âmbito da política estratégica da Rússia no século XXI. Nesse sentido, a pergunta de partida é: *a partir de qual sistemática estratégica a Rússia emprega recursos de poder cibernético?*

Como objetivo geral esse trabalho pretende analisar como os recursos de poder cibernético são utilizados pela Rússia como parte da sua estratégia de defesa. Por sua vez, os objetivos específicos são os listados a seguir:

i. Estabelecer uma fundamentação teórica que considere a associação entre os conceitos de poder cibernético, a securitização e instrumentalização do ciberespaço e a relação entre a guerra moderna e a tecnologia.
ii. Analisar as questões políticas e econômicas internas da Rússia no período pós-soviético até a atualidade.
iii. Examinar as políticas externa, de segurança e de defesa russas.

iv. Compreender como os recursos cibernéticos são trabalhados pela Rússia nos contextos estratégicos, tático e operacional.
v. Analisar os casos da Estônia, Geórgia, Ucrânia e EUA verificando como a estratégia russa se comportou nesses episódios.

Tendo em vista a delimitação do problema, a metodologia de pesquisa implementada foi a exploratória, uma vez que o objetivo das pesquisas exploratórias é "de proporcionar visão geral, de tipo aproximativo, acerca de determinado fato. [...] O produto final deste processo passa a ser um problema mais esclarecido, passível de investigação mediante procedimentos mais sistematizados" (GIL, 2008, p. 27). No caso deste trabalho, o intuito é fornecer novas perspectivas e aprofundamentos teóricos e práticos que auxiliem no entendimento de como o ciberespaço pode ser utilizado pelos Estados nacionais como um novo espaço para a concretização de seus interesses nacionais e para a construção de capacidades assimétricas e ofensivas de combate. Em especial, este estudo também busca auxiliar na compreensão das ações e comportamentos da Rússia no cenário internacional, dados os mais recentes acontecimentos em matéria cibernética, como também de política internacional.

O método de abordagem utilizado é o hipotético-dedutivo, o qual segundo Marconi e Lakatos (2003, p. 106) "se inicia pela percepção de uma lacuna nos conhecimentos, acerca da qual formula hipóteses e, pelo processo de inferência dedutiva, testa a predição da ocorrência de fenômenos abrangidos pela hipótese". Como técnica de investigação foi empregado o método comparativo, que "procede pela investigação de indivíduos, classes, fenômenos ou fatos, com vistas a ressaltar as diferenças e similaridades entre eles" (GIL, 2008, p. 16). Neste trabalho, o método comparativo serviu para analisar os casos de exercício de poder cibernético por parte da Rússia, objetivando-se identificar como a abordagem do país se comportou em determinados contextos e estabelecer o caráter geral da sistemática estratégica que embasa o uso de recursos de poder cibernético.

Dado que a perspectiva deste trabalho é de uma análise de questões político-estratégicas, sendo o componente quantitativo de difícil mensuração, devido ao contexto de escassez de dados disponíveis que poderiam sustentar diagnósticos a partir de outras lentes analíticas, optou-se por limitá-lo a uma pesquisa qualitativa.

Em adição, o estudo se fundamentou em extensa pesquisa bibliográfica, a partir do levantamento e análise de documentos oficiais russos, relatórios técnicos na área de cibernética, bem como de livros acadêmicos e artigos científicos. A seleção da bibliografia se deu a partir da investigação prévia dos elementos centrais que são examinados, isto é, procurou-se primeiramente construir um arcabouço teórico para basear a análise posterior da política estratégica russa, assim como do emprego dos recursos de poder cibernético como instrumentos de defesa.

A hipótese principal que sustenta a pesquisa é a de que a Rússia emprega determinados recursos cibernéticos de acordo com uma abordagem estratégica que busca a desestabilização interna do inimigo, a incapacidade de reação e a dissuasão, a partir de uma retórica defensiva. Também fazem parte desse arquétipo outros recursos, como o econômico, o diplomático e o militar, contudo este trabalho enfatiza a relação entre o elemento cibernético e o militar dessa estratégia.

Em grau secundário, se pressupõe que a escolha para o emprego desses diferentes meios dependa diretamente do país que a Rússia pretenda atacar. Conforme será apresentado, a Rússia possui um objetivo claro de restaurar o seu poder internacional, sem que para isso tenha que se envolver em conflitos cinéticos de larga escala contra países militar e economicamente mais capazes. Portanto, os recursos cibernéticos russos são aplicados de acordo com o poder relativo do país-alvo, sendo por vezes utilizados de maneira coercitiva em conjunto com operações militares e, em outras ocasiões, empregados de forma mais sútil e menos aparente, sem o envolvimento de meios cinéticos.

Este trabalho está dividido, além dessa introdução, em três capítulos de desenvolvimento, um de conclusão e dois anexos. O Capítulo 2 trata sobre o arcabouço teórico necessário para a compreensão acerca da concepção do poder cibernético a partir das teorias neorealista e construtivista das relações internacionais e sobre a relação entre a tecnologia e a guerra, de modo a apresentar uma fundamentação teórico-analítica sobre como o ciberespaço se tornou um ambiente a ser securitizado e utilizado instrumentalmente no âmbito da guerra. Nesse sentido, o poder cibernético é colocado sob as expressões *hard* e *soft*, tendo em vista a dualidade da abordagem russa, analisada no capítulo seguinte.

Em seguida, no Capítulo 3, a política estratégica da Rússia para o século XXI é apresentada e analisada, abordando-se considerações relativas ao ambiente interno do país nos últimos 30 anos, desde o fim da União das Repúblicas Socialistas Soviéticas (URSS). Em adição, são analisados os

aspectos das políticas externa, de segurança e defesa do país, de modo a prover um embasamento contextual sobre como a Rússia observa as suas relações com outros atores e com a própria estrutura do sistema internacional, assim como essas interações se relacionam com os interesses nacionais russos.

Ainda no Capítulo 3 são apresentadas e esquematizadas as capacidades cibernéticas russas, a partir do exame que considera a atuação de suas agências de segurança e de inteligência, da mídia estatal e outras instituições não pertencentes à burocracia oficial russa, que são relacionadas aos objetivos políticos do Kremlin relativos ao uso do espaço cibernético. Logo, todos esses elementos passam ser compreendidos no âmbito da doutrina militar-estratégica russa, que no nível operacional faz referência ao que é chamado de guerra híbrida, no qual os elementos cibernéticos têm participação fundamental.

Finalmente, o Capítulo 4 trata da parte empírica da metodologia. Nele são expostos e analisados quatro diferentes episódios em que a Rússia teria exercido seu poder cibernético contra determinados países. Para o objetivo proposto nesse trabalho, foram escolhidos os casos da Estônia (em 2007), da guerra Russo-Georgiana (em 2008), da crise ucraniana (iniciada em 2013 e presente até os dias atuais) e da interferência na eleição presidencial dos EUA (em 2016).

A escolha dos quatros casos supramencionados deriva especialmente do aparente emprego de recursos cibernéticos por parte da Rússia, de acordo com abordagens e aspectos que diferem em termos qualitativos. Enquanto, por um lado, nos casos da Estônia e dos EUA houve a utilização exclusiva de instrumentos não-cinéticos, nos episódios da Geórgia e da Ucrânia observou-se o emprego de recursos cibernéticos acompanhados de operações militares convencionais. Por fim, o conteúdo presente no Capítulo 4 demonstra que todos esses episódios estão relacionados no âmbito da política estratégica da Rússia e que o emprego de recursos cibernéticos obedece à essa lógica.

2 PODER CIBERNÉTICO E A RELAÇÃO COM A GUERRA MODERNA

Este capítulo trata sobre a fundamentação teórica do trabalho. Nesse sentido coloca-se sob perspectiva como o poder cibernético pode ser empregado como um instrumento de defesa pelos Estados. Para tanto, o capítulo inicialmente versa sobre a conceituação de poder nas relações internacionais sob a ótica das teorias neorealista e construtivista.

Em seguida, é trabalhada a definição de espaço cibernético, a interdependência entre esse novo domínio e a sociedade moderna, a securitização desse domínio pelos Estados e, finalmente, como o arcabouço teórico de poder cibernético apresentado pode ser instrumentalizado por meio de recursos do ciberespaço, nas expressões *hard* e *soft*. Por fim, a relação entre a guerra e a tecnologia é colocada explorada, objetivando tratar sobre o papel do ciberespaço em termos estratégicos e táticos na condução da guerra moderna, principalmente na forma de guerra de informação.

2.1 O PODER

O poder é um conceito-chave no estudo das relações internacionais, uma vez que as relações entre Estados e outros atores do sistema internacional é fundamentada, sob algumas perspectivas teóricas, em relações de poder. Nesse sentido, pretende-se explorar como o poder cibernético pode ser entendido no âmbito das relações internacionais. Porém, inicialmente, são discutidas algumas definições de poder de acordo com autores do campo da ciência política, para depois introduzir o tema no âmbito das relações internacionais. Ao final é apresentado o entendimento desse trabalho sobre como as teorias neorealista e construtivista oferecem um arcabouço teórico e analítico para estudar as características de emprego do poder cibernético para fins de defesa dos Estados.

2.1.1 Poder na Ciência Política

O conceito de poder, assim como diversas outras concepções teóricas no campo das ciências sociais, não pode ser resumido e entendido somente através de uma definição simplória. Existem variadas teses e conceituações sobre a questão do poder, sendo a de Max Weber uma das mais

conhecidas e utilizadas como exemplificação para o debate. Weber define poder como sendo "qualquer chance em uma relação social de impor a vontade de alguém contra a resistência dos outros, independentemente do que dá origem a essa chance" (WEBER, 1922, apud GUZZINI, 2017, p. 100, tradução própria). De acordo com Jordan (1999), Weber entende o poder no sentido de se obter a posse sobre algo ou alguém, sendo a percepção do exercício do poder percebida sempre que se verifica a geração de seus efeitos, sem se preocupar necessariamente com o meio pelo qual esse poder é gerado.

Já Barry Barnes (1988), segundo Turner (1989), por outro lado, entende o conceito de poder a partir da perspectiva da ordem social, isto é, segundo o autor, o poder deriva das estruturas que conformam a sociedade. Barnes acredita que as estruturas sociais são edificadas e modificadas por meio da distribuição do conhecimento que atravessa a sociedade, o qual difunde e determina o caráter normativo e rotineiro pelo qual as pessoas devem agir e se comportar. Jordan (1999), complementa, defendendo que para Barnes a centralidade da problemática do poder é a compreensão de como a ordem social é mantida, de que maneira o poder é capaz de oprimir e reprimir a sociedade.

Outra definição do conceito de poder pode ser encontrada nas obras de Michel Foucault. De acordo com Lamaziere (2009), para Foucault (1995) o poder é um fenômeno essencialmente de dominação, sendo uma força que constitui ordenações desiguais nas relações entre os humanos, em que um dos lados é submetido ao outro. Contudo, diferentemente da concepção de Weber, que enxerga o poder como uma possessão, Foucault percebe que o sentido de dominação pelo poder deriva de como se organizam as instituições que formam a sociedade, que imprimem noções, identidades e normativas ao indivíduo, sujeitando-o seja por controle ou por dependência da estrutura. A leitura trazida por Foucault compreende o poder como uma força indissociável do fenômeno da violência, ainda que o exercício da dominação nem sempre esteja ligado ao emprego da força física (LAMAZIERE, 2009).

Sendo a questão do poder um importante elemento de discussão e conceptualização na Ciência Política, o mesmo se aplica ao campo das Relações Internacionais, tendo em vista que o alicerce teórico da área se preocupa essencialmente em explicar e analisar as dinâmicas que ocorrem no sistema internacional, constituído sobretudo por unidades políticas conhecidas como

Estados nacionais, mas também por outros grupos políticos presentes nas sociedades e que também possuem influência no sistema.

2.1.2 Poder no realismo e no construtivismo

Diferentes interpretações sobre o conceito de poder também são encontradas nas correntes teóricas do campo das relações internacionais, das quais as das teorias realista e construtivista servem como alicerce analítico para o cumprimento dos objetivos deste trabalho. Não obstante a apresentação do conceito de poder para essas duas teorias das relações internacionais, cabe inicialmente uma breve sintetização do teor conceitual central expressado pelo realismo e pelo construtivismo, tendo em vista que todas as teorias de relações internacionais partilham de um mesmo objeto de estudo que é o da relação entre agente, processo e estrutura social (WENDT, 2013).

O realismo, essencialmente, pressupõe a existência de um sistema internacional constituído a partir de uma estrutura anárquica que constrange a discricionariedade de atuação dos atores internacionais, os quais são prioritariamente os Estados nacionais westfalianos (WALTZ, 2010).

Os Estados estão imersos em um ambiente internacional em que esses nunca possuem plena certeza sobre as intenções e presunções dos outros atores internacionais, o que implica em uma incerteza tanto sobre possíveis atitudes benignas quanto hostis, que inclusive podem mudar de caráter rapidamente. Dado os propósitos fundacionais do Estado nacional, a atividade dos atores no sistema internacional caracteriza-se pela busca pela sobrevivência, sendo essa a principal motivação dos Estados, visto que sem a garantia da sobrevivência todos os demais propósitos da existência dessa personalidade jurídica tornam-se impossíveis de serem concretizados. Para os realistas, os Estados são entidades racionais, isto é, deliberam e agem estrategicamente na arena internacional, sempre adotando posturas e ações que indiquem a maximização das possibilidades de sobrevivência. Por fim, os Estados são dotados de capacidades militares que os possibilitam atingir e/ou destruir uns aos outros. Desse modo, os Estados percebem que a forma mais eficaz de operar no cenário internacional é procurando ampliar o seu poder relativo, almejando o ponto em que consigam se tornar o poder hegemônico (MEARSHEIMER, 2001).

Contudo, o realismo não é uma teoria única, podendo ser subdivido conforme determinadas aproximações analíticas, ainda que as premissas sejam as mesmas: o caráter anárquico do sistema internacional e a política internacional baseada nas relações de poder. Para os fins propostos desse trabalho será adotada como base teórica o realismo estrutural – ou neorealismo – dada a abordagem mais ampla no que tange a análise dos atores e das formas de desempenho do poder internacional.

Já o construtivismo, que aparece como uma teoria alternativa ao debate clássico na área entre realistas e liberais, alicerça as suas bases conceituais para explicar as relações internacionais na questão da construção social da subjetividade. Para os teóricos construtivistas, as dinâmicas sociais, e isso inclui as relações internacionais, são formadas por meio de interpretações normativas e epistêmicas derivadas das interações humanas. Desse modo:

> Os construtivistas acreditam que as relações internacionais consistem primariamente em fatos sociais, os quais são fatos apenas por acordo humano. Ao mesmo tempo, os construtivistas são "realistas ontológicos"; acreditam não apenas na existência do mundo material como que "esse mundo material oferece resistência quando agimos sobre ele" (Knorr Cetina, 1993: 184). Assim, o construtivismo é uma tentativa, mesmo que tímida, de construção de uma ponte entre as intensamente separadas filosofias da ciência social positivista/materialista e idealista/interpretativista (ADLER, 1999, p. 206).

Na teoria construtivista, as ideias – compreendidas como o conhecimento coletivo reconhecido por meio de práticas – formam a capacidade e a motivação da ação social. Nesse sentido, as práticas operacionalizadas por meio do conhecimento coletivo são originárias das interações entre os indivíduos inseridos na sociedade, os quais agem conforme suas ideologias, crenças e interpretações individuais. Dessa forma, e replicando o entendimento construtivista para o cenário internacional, tem-se que a atuação dos Estados é baseada nas percepções que esses desenvolvem sobre os demais atores internacionais e sobre a estrutura do sistema, a partir das concepções interpretativas do mundo material geradas através de cada uma das sociedades nacionais (WENDT, 1999).

Portanto, há diferenciação relevante entre, de um lado, a perspectiva realista de um sistema internacional imutável e de uma estrutura impositiva, e de outro, a noção construtivista que essas concepções nada mais são do que resultado de "realidades" socialmente construídas com base nas interações dentro das sociedades nacionais.

O poder na teoria realista é um termo central, visto que para os realistas a política de poder é uma característica substancial no entendimento das relações internacionais, principalmente quando se trata do estudo da política internacional no âmbito das relações entre as grandes

potências (MORGENTHAU, 2003). A compreensão do poder para os realistas está intimamente ligada ao conceito de poder como uma forma de dominação do outro, atrelando-o ao interesse e a força dos Estados, sendo a interpretação de que esse poder é exercido essencialmente de maneira coercitiva – denominado de *hard power*.

A definição de poder para os realistas também está orientada com a capacidade de exercer influência dos Estados no cenário internacional, com a observação da capacidade de um Estado em exercer essa influência, no âmbito de uma atuação em termos de política de poder – ou *Realpolitik* - quando há uma reserva significativa de recursos de poder coercitivo, de matiz tipicamente militar. Isso inclui, na visão realista neoclássica:

> [...] uma população densa juntamente com um território vasto e estrategicamente posicionado é de grande relevância para a manifestação e consolidação do poder em seu sentido amplo (já abordado anteriormente neste livro). Nesse ponto, é importante salientar que uma eficiente capacidade produtiva do complexo comercial-industrial e bélico, de tecnologia com habilidade para desenvolver armamentos militares avançados, objetivando a defesa nacional e a geoestratégia de integridade territorial, que inclui doutrina militar, traz pontos de reforço no realismo neoclássico. No plano da manutenção e defesa da integridade territorial – máximas do realismo neoclássico – do Estado contra o inimigo externo, é fundamental entabular forças armadas, especialmente, de pronto emprego para defesa e/ou ataque estratégicos. As forças armadas de um Estado em condições de vulnerabilidade e de cobiça internacionais devem exercer papel importante na análise global de longo curso de seus objetivos geopolíticos (CASTRO, 2012, p. 326).

Nota-se, portanto, que mesmo que o exercício do poder, na concepção realista, não esteja sempre ligado à prática da violência física, o poder militar como força de mobilização, de intimidação e de dissuasão é tido como primordial para que um Estado tenha sucesso na sua estratégia de projeção de poder no cenário internacional (CASTRO, 2012).

Abaixo, o Quadro 1 apresenta as diferentes estratégias que os Estados podem utilizar para captar poder na arena internacional, de acordo com a visão de John J. Mearsheimer, que pertence ao que se denomina “realismo ofensivo”.

Quadro 1 – Estratégias dos Estados

Strategies for gaining power	
War	May be efficient but costly
Blackmail	Cost efficient but ineffective against great powers
Bait-and-bleed	Cost efficient but difficult to bait rivals into conflict
Bloodletting	Cost efficient but riskof exposure

Fonte: Toft (2005, p. 385).

No que concerne ao aspecto da maximização do poder relativo, ação primordial na atuação estratégica dos Estados, Mearsheimer (2001) expõe que a guerra é a principal forma de aumentar o poder estatal. Contudo, entende-se que a guerra pode ser muitas vezes custosa, por isso outras ações como a utilização de chantagem para a obtenção de ganhos relativos por meio da ameaça e, com isso, da realização de concessões pelo inimigo; ou a realização de ações, por um Estado A que procurem enganar outros Estados, envolvendo-os, por exemplo, em conflitos que gerem desgastes entre eles, enquanto o Estado A consegue fortalecer a sua posição de poder (TOFT, 2005).

De forma geral, percebe-se que a obtenção e o exercício do poder na concepção realista estão muito relacionados com a geração de capacidades materiais, especialmente militares e econômicas, para fins de promoção de influência no cenário internacional de forma coercitiva, buscando o aumento do poder relativo. Embora algumas correntes dentro do realismo também reconheçam o exercício do poder por meios não coercitivos, como, por exemplo, meios de controle e manipulação da opinião pública, na concepção de *soft power*, não é admitida uma dissociação entre os recursos de *soft* e de *hard power*, dado que os elementos coercitivos são fundamentais para o aumento de poder relativo, colocando-os hierarquicamente acima dos instrumentos de *soft power* (SCHMIDT, 2007).

Em contrapartida, o conceito de poder para os construtivistas reside menos na concepção isolada de capacidades geradas por recursos materiais e mais em uma compreensão de poder relacional. Desse modo, o construtivismo acredita que a obtenção e o exercício do poder dependem das dinâmicas relacionais entre dois ou mais atores internacionais e de qual é a percepção que cada um possui dos demais. Como exemplo, Guzzini (2010) menciona que a capacidade ofensiva dos mísseis nucleares franceses não são uma ameaça para Luxemburgo, uma vez que a relação que os dois países possuem é baseada na confiança.

> A *fortiori*, o construtivismo não é propenso a repetir o que Robert Dahl uma vez chamou de falácia do poder, onde todos os possíveis recursos de poder seriam misturados e adicionados. Essa avaliação agregada do poder (recurso), independentemente dos entendimentos do ator e do cenário situacional contingente, não seria apenas errada, mas conceitualmente impossível (GUZZINI, 2010, p. 12, tradução própria).

.

Ainda que o conceito clássico de poder, utilizado pelos realistas, entendido como a capacidade submeter um Estado aos interesses de outro sem que esse assim o deseja, não seja totalmente dispensado pelos construtivistas, o foco da análise nesse caso é mais direcionado ao

conhecimento e percepção social que permeia a relação entre os dois Estados, e não somente em termos de recursos. Nessa perspectiva, Guzzini (2010) acrescenta:

> No entanto, a teorização construtivista daria um toque comunicativo a isso, insistindo no papel do reconhecimento aberto ou tácito que, por sua vez, depende de um contexto social ou cultural mais amplo. Esse reconhecimento é tipicamente baseado em convenções, pois, como mencionado acima, os recursos recebem peso não por si mesmos, mas por entendimentos compartilhados nas relações sociais, e também porque o reconhecimento de um status geral de poder é social. Assim como as comunicações individuais fazem parte e fazem sentido no contexto de uma linguagem como um todo, o aspecto relacional do poder é concebido dessa maneira mais ampla, de modo a permitir que as normas sociais se tornem visíveis em seu papel na avaliação do poder como autoridade (GUZZINI, 2010, p. 13, tradução própria).

Em lógica similar, Wendt (2013) ao trabalhar sua crítica ao entendimento da estrutura anárquica do sistema internacional descrita por realistas como Waltz, tece sua compreensão sobre como as instituições e as identidades formuladas por meio da interação social resultam em percepções e julgamentos sobre o "outro". Tal assimilação permite aferir, por exemplo, que a noção da política de poder como cerne da política internacional nada mais é do que uma concepção baseada em termos interpretativos e sociológicos, e não uma característica sistêmica imutável.

2.1.3 Poder Cibernético à luz do realismo e construtivismo

Na concepção realista, o ciberespaço nada mais é do que um novo ambiente operacional para a atuação dos Estados, assim como os espaços terrestre, aéreo e marítimo. Portanto, a atividade dos atores no ciberespaço é baseada na busca pela projeção de poder e influência sobre os demais, fazendo uso dos recursos disponíveis, gerando uma constante tendência em securitizar esse espaço (ACÁCIO, 2016). Essa interpretação está escorada na conceitualização realista sobre a imutabilidade das premissas que constituem o sistema internacional, bem como da relação entre o agente e a estrutura.

Clarke e Knake (2015), ditos alinhados aos princípios neorealistas, defendem que são os Estados os mais interessados e habilitados a desenvolver capacidades cibernéticas, de modo a concretizarem os seus interesses nacionais no ciberespaço. Nessa perspectiva, os autores apresentam a visão de que o exercício do poder cibernético se dá prioritariamente por meio da guerra cibernética, empregando as capacidades computacionais do ciberespaço para fins políticos.

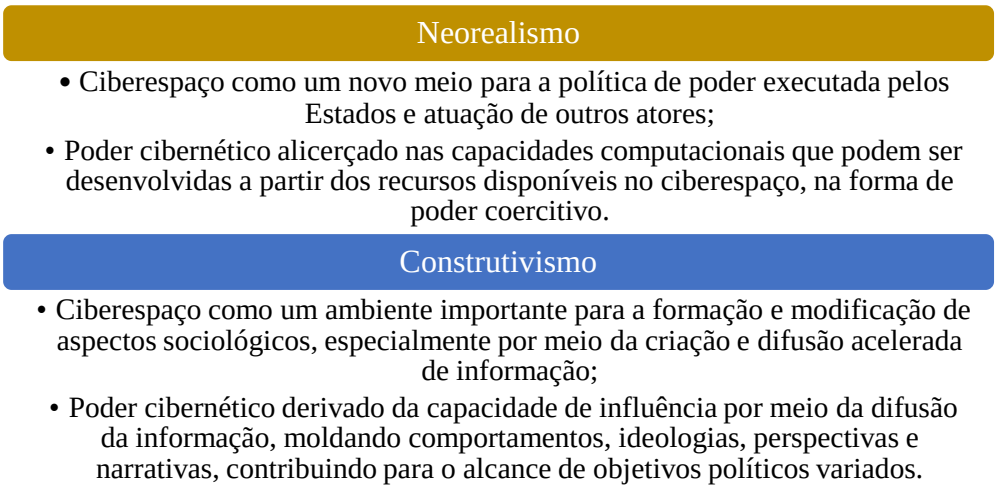
Enquanto, por um lado, o realismo observa o ciberespaço como um novo meio para o alcance de um fim imutável: o exercício da política de poder. A partir das leituras de Wendt (1999),

Adler (1999) e Guzzini (2010), pode-se assimilar que o construtivismo apresenta uma análise mais ampla do papel do ciberespaço para a agenda nacional, podendo ser destacado a importância do elemento informacional que ganhou novas proporções com o advento das soluções da Tecnologia da Informação e Comunicação (TIC) e, especialmente nesse sentido, com a invenção da Internet e das mídias de massa.

Portanto, o ciberespaço, ao contribuir com a difusão rápida e amplificada da informação, se torna um importante meio indutor e moldador de comportamentos, percepções, narrativas e ideologias. Logo, na perspectiva construtivista, o interesse dos Estados em relação ao ciberespaço está relacionado a capacidade de influenciar outras unidades políticas por meio da manipulação dos elementos informacionais, podendo ser considerada uma dimensão *soft* do poder cibernético.

A Figura 1 expõe uma síntese das principais diferenças de abordagem sobre o poder cibernético para o (neo)realismo e o construtivismo.

Figura 1 – Síntese da compreensão do poder cibernético a partir das teorias neorealista e construtivista



Fonte: Elaboração própria com base nas leituras de Waltz (2010), Mearsheimer (2001), Castro (2012), Wendt (1999) e Adler (1999).

Tendo em vista a absorção de um melhor entendimento sobre como ambas as teorias expostas e as suas contribuições para a análise do poder cibernético são essenciais para a concretização dos objetivos desse trabalho, a seguir são explorados os aspectos estruturais do ciberespaço que o torna tão relevante para a ótica de segurança e defesa dos Estados.

2.2 EXERCÍCIO DO PODER NO ESPAÇO CIBERNÉTICO: RECURSOS E DIMENSÕES

O ciberespaço emergiu como um novo domínio de atuação humana. As soluções de tecnológica da informação e comunicação (TIC), principalmente na forma de sistemas de informação criaram uma interdependência (ou dependência) entre a sociedade e seus setores com o ciberespaço. Além disso, a utilização do ciberespaço por meio das mídias de informação e redes sociais pelos indivíduos para se informar, contribuiu para que esse ambiente se torna-se fundamental para a construção de ideologias, narrativas, discursos e movimentos político-sociais.

Da mesma forma, os Estados passaram a implementar medidas para securitizar o ciberespaço e utilizar seus recursos como instrumentos de defesa, dados os aspectos estratégicos desse domínio. Este subcapítulo explora essas questões, inicialmente estabelecendo o escopo de análise do ciberespaço desse trabalho e em seguida discutindo as características e dinâmicas do ciberespaço que são relevantes para a decisão dos Estados em securitizar o domínio. Por fim, as conclusões relativas ao poder cibernético são interligadas aos recursos do ciberespaço, de modo a oferecer duas expressões dos recursos cibernéticos: uma *hard*, que compreende medidas coercitivas; e outra *soft*, que compreende medidas de influência não-coercitiva.

2.2.1 Definição de espaço cibernético

Até mais recentemente, as sociedades humanas desenvolveram suas atividades em dois domínios físicos: o terrestre e o marítimo. Entretanto, e especialmente no caso do ambiente marítimo, esses espaços só puderam ser utilizados de forma mais aprimorada a partir do desenvolvimento e utilização de tecnologias de locomoção e transporte. Foi inclusive com o progresso da tecnologia e com as inovações nos meios de produção e nas áreas da engenharia que o ser humano conquistou o terceiro domínio físico, o ar, no início do século XX.

Após a conquista do domínio aéreo e com a continuidade das pesquisas e desenvolvimento de tecnologias aeronáuticas, não demorou para que a humanidade conseguisse chegar ao espaço sideral – o quarto domínio físico - e iniciar uma nova era de descobertas científicas que, por sua vez, deram novo impulso para o progresso tecnológico.

Contudo, diferentemente dos domínios anteriormente citados – terrestre, marítimo, aéreo e espacial – existe uma maior discordância na literatura sobre a definição do ciberespaço. Enquanto

os demais podem ser mais facilmente delimitados e concebidos, inclusive no senso comum, o ciberespaço possui algumas características que dificultam a sua demarcação e acepção.

Dentre as diversas definições sobre ciberespaço presentes na literatura, desde especialistas em computação e telecomunicações até políticas e planos nacionais sobre cibernética, a provida por Kuehl (2009) pode ser considerada como uma das mais amplas sobre o tema. Segundo o autor:

> [...] ciberespaço é um domínio global dentro do ambiente de informação cujo caráter distinto e único é enquadrado pelo uso da eletrônica e do espectro eletromagnético para criar, armazenar, modificar, trocar e explorar informações por meio de redes interdependentes e interconectadas usando tecnologias de comunicação e informação (KUEHL, 2009, s/p, tradução própria).

Ainda de acordo com o autor, é demasiado limitador dispor que o ciberespaço se baseia somente em um ambiente "digitalizado e computadorizado" (KUEHL, 2009, s/p). Nessa concepção, uma série de tecnologias poderiam ser citadas como integrantes do ciberespaço, como as tecnologias que fazem parte do *Global Positioning System* (GPS) e das radiocomunicações em geral, uma vez que são constituídas por equipamentos eletrônicos que fazem uso do espectro eletromagnético para transmitirem informações.

Apesar da ampla definição trazida por Kuehl (2009) ser importante para a problematização do ciberespaço, especialmente do ponto de vista securitário, o entendimento que é utilizado como fundamento nesse trabalho para o cumprimento dos objetivos elencados, é mais próximo da definição trazida por Singer e Friedman (2013) e complementada por Clarke e Knake (2015).

Para Singer e Friedman (2013) o domínio cibernético é, essencialmente, um ambiente informacional. Nesse espaço a informação é criada, armazenada e disseminada através de um ambiente digital, suportado por infraestruturas físicas existentes em diversas localidades do globo. Desse modo, o espaço cibernético pode ser definido como a confluência entre redes de computadores, dispositivos eletrônicos e infraestruturas de telecomunicações interligados por onde trafegam informações de modo virtual. Ele é constituído por elementos virtuais/digitais (informações) e por elementos físicos (computadores, servidores, cabos de fibra ótica, comutadores, modems, entre outros).

Por sua vez, Clarke e Knake (2015) mostram que a interconexão entre as diferentes redes de computadores, por meio das infraestruturas de telecomunicação, forma o que é conhecido por *World Wide Web* – ou simplesmente Internet. Contudo, ainda segundo os autores, o ciberespaço não é somente constituído pela Internet, mas também é formado pelas redes de computadores

privadas, as quais, em tese, não estão conectadas com a Internet. Essas redes privadas são comuns nos ambientes virtuais internos de empresas, entidades, órgãos e agências governamentais e dos sistemas de controle das infraestruturas críticas, detalhadas mais adiante.

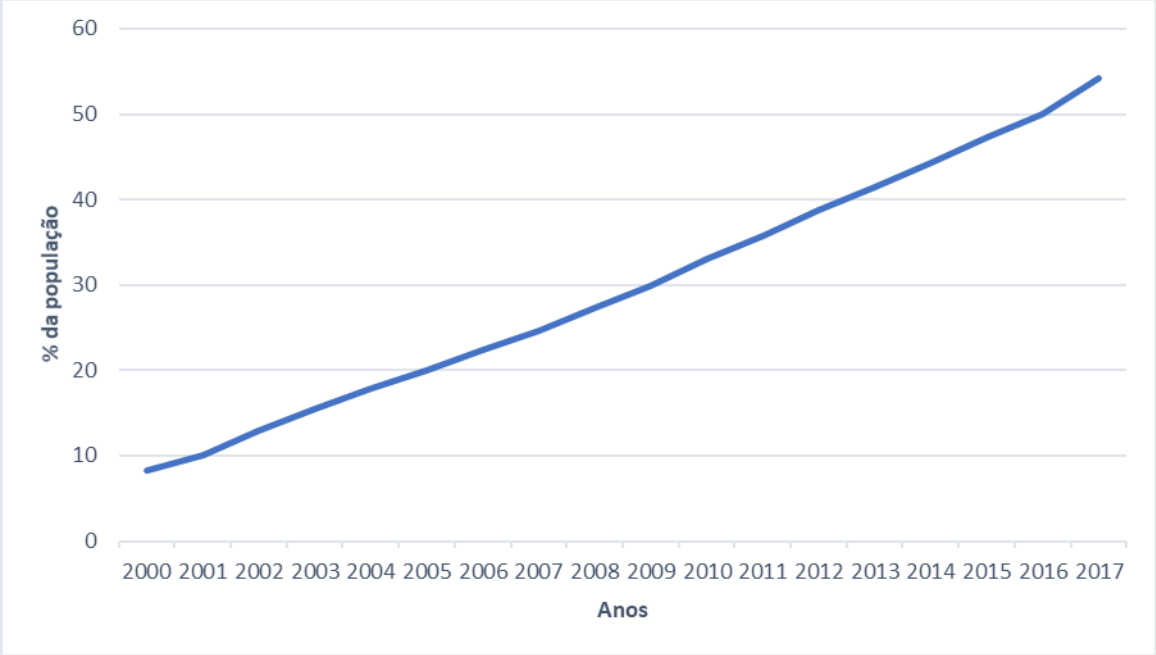
De acordo com Ventre (2019), o ciberespaço pode ser também compreendido a partir de um modelo de três dimensões, onde:

> Uma primeira camada é constituída pela arquitetura material, física, *hardware*; ela é feita pelo conjunto de computadores, calculadoras, cabos eletrônicos (*hardware layer*). Uma segunda camada, média, denominada *software* ou aplicativa, é constituída pelo conjunto de programas, códigos, dados e algoritmos que dão vida ao ciberespaço (*software layer*). E uma terceira camada, informacional, é a do sentido, das informações (*news*), dos conteúdos (*meatware layer*) (VENTRE, 2019, p. 77).

A compreensão do ciberespaço segundo as três dimensões sintetizadas por Ventre (2019) permite analisar esse domínio a partir de aspectos técnico-computacionais (dimensões de *hardware* e *software*) e aspectos sociológicos e psicológicos (dimensão humana).

A seguir, a Gráfico 1 apresenta a evolução do percentual médio global de pessoas utilizando a Internet. Nota-se que o número de indivíduos utilizando a Internet segue uma tendência de crescimento sustentado ao longo do tempo, com características de progressão aritmética.

Gráfico 1 - Indivíduos utilizando a Internet no mundo em percentual da população (2000-2017)

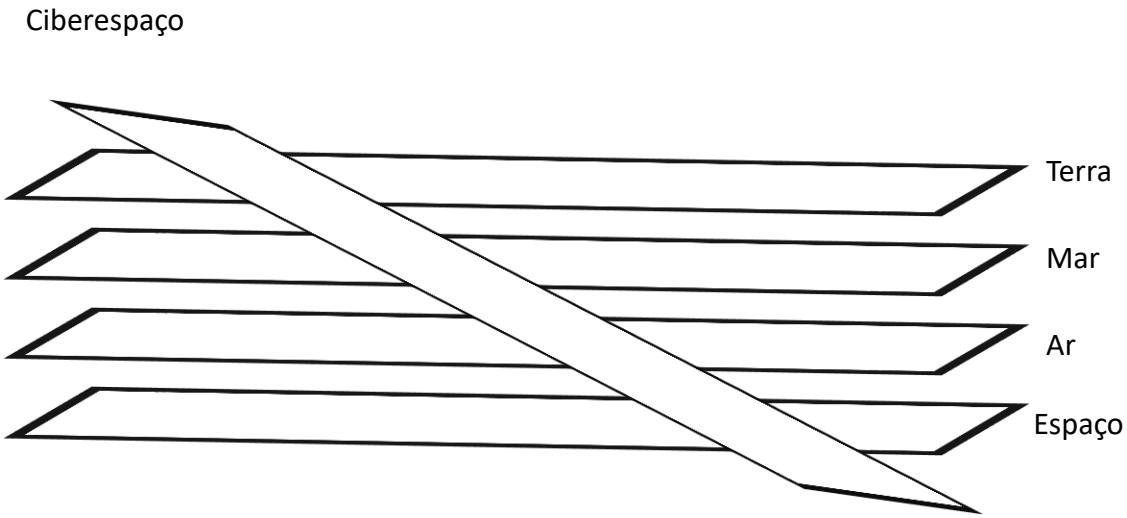


Fonte: World Bank (2020).

O desenvolvimento das tecnologias da informação e comunicação (TIC) - que servem de base para a existência do ciberespaço e o compõem – e a sua introdução cada vez mais aparente na vida cotidiana das pessoas, gera interferências nas dinâmicas sociais, políticas e econômicas que moldam não somente os aspectos técnicos do ciberespaço, mas igualmente as regras que são criadas para a regulamentação desse meio. Aqui cabe mencionar a importante diferença do ciberespaço para os demais domínios de atuação humana (terra, água, ar e espaço): enquanto os ambientes geográficos são naturais e não permitem alterações substanciais de suas formas, o ciberespaço é um domínio artificial, criado pelo homem e por ele moldável, tanto em sua composição quanto em seus fins e, por ser virtual, permeia todos os demais domínios (NYE, 2010; NETO, 2014).

A Figura 2 expõe a relação que o ciberespaço possui com os domínios geográficos tradicionais, fazendo alusão a como as dinâmicas produzidas no interior do ciberespaço podem produzir efeitos diretos ou indiretos sobre os demais domínios.

Figura 2 – Aspecto de transversabilidade do ciberespaço em relação aos demais domínios

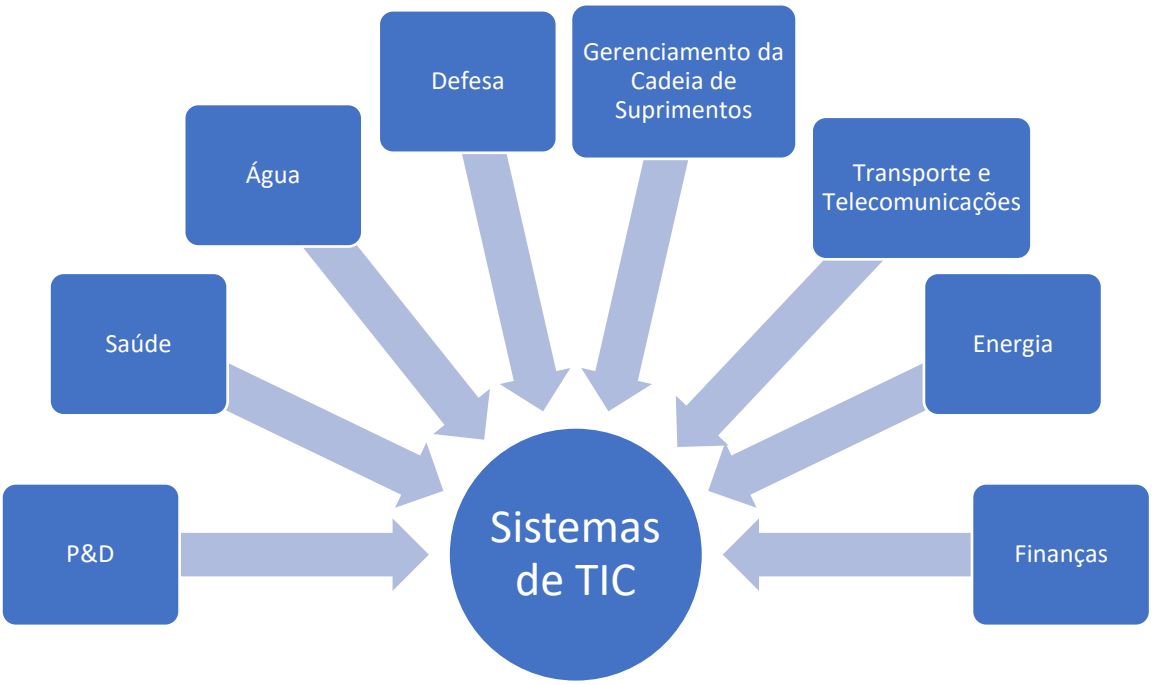


Fonte: Adaptado de Ventre (2012, p. 35).

A transversabilidade do ciberespaço em relação aos demais domínios é um resultado da constante e cada vez maior interdependência entre a sociedade civil e as soluções de TIC. Essa interdependência é notável ao se verificar o quantitativo de setores da sociedade que atualmente

possuem algum grau de dependência de sistemas informatizados, seja para o processamento de dados e informações ou para o controle direto ou indireto, total ou parcial, de infraestruturas públicas e privadas. A Figura 3 apresenta essa interdependência.

Figura 3 – Interdependências entre os sistemas de TIC e os setores da sociedade



Fonte: Adaptado de Ghernaouti (2013).

Nessa perspectiva, é notável que o ciberespaço seja percebido pelos Estados como um novo domínio em que as relações domésticas e internacionais se desenvolvem nas áreas sociais, culturais, comerciais, financeiras e políticas. Ainda que essas relações também se desenvolvam de forma física nos domínios geográficos tradicionais, as dinâmicas humanas são intensificadas no meio cibernético, tendo em vista a capacidade de comunicação praticamente imediata, a difusão de informações em escala global a partir de poucos recursos e a realização de atividades de maneira remota. A interdependência dessas instituições e dos setores da sociedade em relação aos sistemas de TIC é algo que, a seguir, será destacado para justificar as preocupações e interesses do Estado com o ciberespaço (GHERNAOUTI, 2013).

Dada a interpenetração do ciberespaço nos campos de atuação humana, cresce a tendência, por parte dos governos, em tratar esse ambiente de maneira estratégica, a partir de uma observação

que identifica a relevância do espaço cibernético para as questões de segurança nacional. Tal circunstância não é inédita, haja vista a elaboração de preceitos teórico-estratégicos para securitização dos domínios terrestre, marítimo e aéreo, inclusive com a organização de forças armadas especializadas em cada um desses espaços geográficos (CLARKE; KNAKE, 2015).

2.2.2 Securitização do espaço cibernético

A preocupação com questões centrais no ciberespaço pelos Estados, abrangem, mas não se limitam a: governança da Internet; localização das infraestruturas de telecomunicação; tráfego de informações; e, vulnerabilidades dos sistemas de controle das infraestruturas críticas (CLARKE; KNAKE, 2015).

O aspecto da governança é relevante, dado que atualmente não está sendo abordada a questão do ciberespaço pela legislação internacional de forma substancial. Aliás, muitos assuntos sobre a matéria permanecem sobre o desamparo de dispositivos normativos internacionais que poderiam pacificar contenciosos, disputas legais e a resolução de atos criminosos cometidos no ciberespaço ou fazendo uso desse meio.

Não há uma entidade internacional, criada sob os auspícios do sistema das Nações Unidas (ONU), incumbida de realizar a regulamentação do espaço cibernético e das relações que ocorrem no meio[1]. Cabe ressaltar a existência de organizações com essa incumbência para os espaços marítimo e aéreo: a Organização Marítima Internacional[2] (OMI) e a Organização da Aviação Civil Internacional[3] (OACI). No que concerne ao domínio terrestre, a legislação internacional sobre o tema é encontrada nos tratados internacionais assinados de forma bilateral ou multilateral (no caso de regras positivadas nos tratados constituintes dos blocos econômicos) (REZEK, 2016).

No que tange a localização das infraestruturas de telecomunicações - ou infraestruturas de suporte – a importância dada pelos Estados, em termos estratégicos, pode ser explicada devido aos processos de funcionamento da Internet e pela questão da territorialização dos elementos físicos que a suportam. Isto é, a localização de infraestruturas, como servidores e cabos de fibra ótica, no território de outros Estados pode representar risco à segurança nacional, uma vez que informações

[1] A *International Telecommunication Union* (ITU) se limita ao estabelecimento de padrões de comunicação que tornam possível que as tecnologias de informação possam operar (ITU, 2020).
[2] Disponível em: http://www.imo.org/en/Pages/Default.aspx.
[3] Disponível em: https://www.icao.int/Pages/default.aspx.

sigilosas podem trafegar sobre outro território soberano. Além disso, um Estado pode bloquear o tráfego que entra ou sai de um outro Estado, limitando seu acesso à internet ou até mesmo interrompendo-o totalmente (CLARKE; KNAKE, 2012).

Com certa correlação com a questão anterior, o tráfego de informações no ciberespaço também preocupa os Estados, tendo em vista que o espaço cibernético pode funcionar como meio para a criação e difusão de informações que fragilizem a segurança nacional ou desestabilizem as instituições de Estado e de governo, seja a partir de pressão externa ou interna. No último caso, a capacidade do meio cibernético em difundir informações, em especial por meio das mídias sociais, pode significar a mobilização da opinião pública para uma causa específica ou incentivar a sua polarização política, atos que podem induzir riscos não somente à estabilidade do governo, mas também à ordem pública (CONNELL; VOGLER, 2017).

Nesse sentido, as mídias sociais são proporcionadoras e catalisadoras desse tipo de artifício político, tanto pela capilaridade das informações presentes, quanto pela influência que esses meios representam na formação de opiniões e tendências na vida do cidadão (AYRES PINTO; MORAES, 2020).

Finalmente, as vulnerabilidades dos sistemas de controle das infraestruturas críticas também são assuntos de interesse do Estado, dado que, como a nomenclatura indica, as infraestruturas críticas são elementos indispensáveis para o devido funcionamento da sociedade civil, da manutenção da ordem pública e para a segurança nacional. Não há uma definição exata de todos os elementos que podem ser definidos como infraestruturas críticas, mas alguns são alvos de maior consenso, por exemplo: redes de captação e abastecimento de água; redes de geração e transmissão de eletricidade; redes de comunicação dos órgãos de emergência; sistemas bancários e financeiros; sistemas de telecomunicação em geral; sistemas de transporte e logística; sistemas de gerenciamento e controle do tráfego aéreo; sistemas de comunicação das forças armadas; sistemas de controle das defesas antiaéreas e das forças de mísseis; entre outros (FERNANDES, 2012).

Essas quatro questões sobre o ciberespaço e a operacionalização das atividades desenvolvidas nesse ambiente, além de levantarem preocupação por parte dos Estados, despertam igualmente o interesse dessas unidades políticas para as possibilidades que o ciberespaço oferece em termos estratégicos. Nesse sentido, os recursos cibernéticos podem ser utilizados para a projeção de poder do país, imprimindo a influência do Estado, por meios coercitivos ou não, além

dos limites próximos à sua fronteira nacional, sem o uso da força militar convencional ou de sanções econômicas. Ademais, os recursos cibernéticos podem auxiliar a concretização de objetivos estratégicos em operações que também sejam empregadas forças militares (CONNELL; VOGLER, 2017). Em suma, os recursos cibernéticos podem servir de diferentes formas às estratégias de segurança e defesa nacionais.

2.2.3 *Hard* e *soft power* cibernético

Nye (2010), um autor neoliberal, faz uma analogia com os domínios geográficos tradicionais para demonstrar como os Estados utilizam uma série de recursos para exercer poder e em como o desenvolvimento de novas tecnologias reflete os domínios de poder, alterando a forma com que as disputas, em nível internacional, ocorrem. De acordo com Nye (2010):

> poder marítimo refere-se ao uso de recursos no domínio dos oceanos para vencer batalhas navais no oceano, controlar pontos de estrangulamento de navios como estreitos e demonstrar uma presença *offshore*, mas também inclui a capacidade de usar esses oceanos para influenciar batalhas, comércio e opiniões em terra. Em 1890, Alfred Thayer Mahan popularizou a importância do poder marítimo no contexto de novas tecnologias de propulsão a vapor, armaduras e armas de longo alcance. O presidente Theodore Roosevelt respondeu ampliando bastante a marinha americana e enviando-a ao mundo em 1907. Após a introdução de aeronaves na Primeira Guerra Mundial, militares começaram a teorizar sobre o domínio do poder aéreo e sua capacidade de atacar diretamente o centro de gravidade urbano de um inimigo sem que os exércitos tivessem que cruzar fronteiras. Os investimentos de Franklin Roosevelt no poder aéreo foram vitais na Segunda Guerra Mundial. E após o desenvolvimento de mísseis intercontinentais e satélites de vigilância e comunicação na década de 1960, os escritores começaram a teorizar sobre o domínio particular do poder espacial. John F. Kennedy lançou um programa para garantir uma liderança americana no espaço e colocar um homem na lua. Em 2009, o presidente Barack Obama solicitou uma nova e importante iniciativa no poder cibernético, e outros governos seguiram o exemplo (NYE, 2010, p. 4, tradução própria).

A exemplificação apresentada pelo autor mostra como as novas descobertas tecnológicas tornaram possíveis novos usos dos domínios geográficos para a projeção de poder dos Estados. Tal constatação é igualmente válida para o ciberespaço, o qual surgiu justamente das inovações nas tecnologias de informação e comunicação, com um processo acelerado de incorporação nas dinâmicas sociais, econômicas e políticas da sociedade (NYE, 2010).

Entretanto, apesar das semelhanças entre os fins últimos do emprego de recursos de poder nas diferentes esferas, algumas particularidades do ciberespaço devem ser ressaltadas, em especial no que tange aos conflitos e a guerra. Em primeiro lugar, nos domínios geográficos tradicionais, os Estados, em regra, possuem o monopólio do uso da força em larga escala, os teatros de batalha

são conhecidos e os ataques costumam cessar por atrito ou exaustão, o que demonstra que a capacidade em movimentar os recursos é custosa. Por outro lado, no ciberespaço - devido às singularidades como a facilidade de acesso ao meio e o elevado fator de anonimidade - existem diversos atores atuantes, a distância física entre o atacante e o alvo é irrelevante e os recursos mobilizáveis são relativamente de baixo custo (NYE, 2010).

Ainda numa análise comparativa com outros domínios de poder, é possível identificar outras correspondências entre os espaços geográficos tradicionais e o espaço cibernético. Nesse sentido, Nye (2010) afirma que o poder cibernético é capaz de afetar diversas esferas, projetando seus efeitos para além do mundo virtual. Assim sendo, o Quadro 2 apresenta exemplos de usos de recursos cibernéticos para exercer poder a partir das perspectivas do âmbito de seus efeitos (intra ciberespaço e extra ciberespaço), bem como, de sua natureza: informacional ou física. Ademais, esses recursos de poder podem ser lidos através de uma concepção de poder *hard* ou *soft*.

Quadro 2 – Dimensões Físicas e Virtuais do Poder Cibernético

	Intra cyber space	Extra cyber space
Information Instruments	**Hard:** Denial of service attacks **Soft:** Set norms and standards	**Hard:** Attack SCADA systems **Soft:** Public diplomacy campaign to sway opinion
Physical Instruments	**Hard:** Government controls over companies **Soft:** Infrastructure to help human rights activists	**Hard:** Bomb routers or cut cables **Soft:** Protests to name and shame cyber providers

Fonte: Nye (2010, p. 5).

A análise do Quadro 2 permite aferir algumas conclusões relevantes sobre os desdobramentos do uso de recursos de poder cibernético. Inicialmente, nota-se que os recursos de informação podem ser empregados para pautar agendas, ditar princípios e gerar resultados por atração e persuasão, realizando *soft power* no âmbito interno do ciberespaço. Um exemplo nesse sentido pode ser o desenvolvimento de um novo padrão de interface de comunicação de *software* que atraia comunidades de programadores para a sua utilização (NYE, 2010).

Da mesma forma, os Estados podem utilizar o ciberespaço para realizar ataques coordenados de *Distributed Denial of Service* (DDoS) por meio do uso de *botnets*[4] de centenas ou milhares de computadores infectados por um vírus de computador. Esses ataques podem ser direcionados para sistemas na Internet de entidades públicas ou privadas, tornando seus serviços em rede inacessíveis e inoperantes (SINGER; FRIEDMAN, 2013). Por representar uma atitude tipicamente coercitiva, pode-se entender que o atacante está gerando *hard power* por meio de instrumentos de informação na esfera do ciberespaço.

Sobre os efeitos nas dimensões físicas, podem ser exemplificados ataques cibernéticos contra sistemas de controle de infraestruturas críticas, de modo a torná-las inoperantes ou causar mal funcionamento, gerando prejuízos para a economia e, dependendo do alvo, para a segurança nacional. Tais ações podem ser executadas, por exemplo, por meio das seguintes técnicas:

- da instalação de um *malware*[5] em um computador que mantenha comunicação com os sistemas de controle;
- da invasão de um sistema de computador diretamente por meio de algum *backdoor*[6] e, a partir daí, alterando parâmetros computacionais nos sistemas de controle;
- da invasão de um sistema de computador por meio do comprometimento das credenciais de segurança, utilizando-se da técnica *spear phising*[7];

[4] De acordo com a Agência da União Europeia para Segurança Cibernética (da sigla em inglês, ENISA), uma *botnet* é "um conjunto de computadores infectados por bots. Um bot é um software malicioso que recebe ordens de um mestre. […] Um computador é infectado quando um *worm* ou vírus instala o bot ou quando o usuário visita um site malicioso que explora uma vulnerabilidade no navegador". Disponível em: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets.

[5] Ainda de acordo com a ENISA, "qualquer software que execute operações indesejáveis, como roubo de dados ou algum outro tipo de comprometimento do computador, pode ser classificado como malware. Malware é um termo amplo que pode se referir a vários tipos de programas maliciosos". Disponível em: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/malware. Acesso em 20 de junho de 2020.

[6] De acordo com Zetter (2014, s/p, tradução própria) "um *backdoor* em um *software* ou sistema de computador é geralmente um portal não documentado que permite que um administrador entre no sistema para solucionar problemas ou fazer manutenção. Mas também se refere a um portal secreto que hackers e agências de inteligência usam para obter acesso ilícito. [...] Frequentemente, a existência do *backdoor* é desconhecida do proprietário do sistema e conhecido apenas pelo fabricante do *software*. *Backdoors* administrativos integrados criam uma vulnerabilidade no software ou sistema que os invasores podem usar para obter acesso a um sistema ou dados."

[7] Segundo a firma especializada em segurança cibernética, Kaspersky Lab, "Spear phishing é um esquema de email ou comunicação eletrônica direcionado a um indivíduo, organização ou negócio específico. Embora muitas vezes tenham a intenção de roubar dados para fins maliciosos, os cibercriminosos também podem ter a intenção de instalar um malware no computador de um usuário-alvo.". Disponível em: https://www.kaspersky.com/resource-center/definitions/spear-phishing. Acesso em 21 de junho de 2020.

- da invasão de um sistema por meio de uma injeção SQL, obtendo-se acesso ao banco de dados do sistema[8].
- da instalação de uma bomba-lógica[9] nos sistemas de controle, objetivando destruir todas as informações presentes no sistema e torná-lo inoperante (CLARKE; KNAKE, 2015).

Atos como esse, exemplificados no Quadro 2 como 'Ataque aos sistemas SCADA', podem significar a implementação de *hard power* pelo Estado atacante. SCADA é a abreviatura para *Supervisory Control and Data Acquisition*, sendo uma combinação de *softwares* e *hardwares* utilizados comumente por organizações industriais para fins de monitoramento dos processos industriais em tempo real, coleta de dados das operações e execução de ações de forma direta em aparelhos e equipamentos industriais (COPADATA, [s.d.]). Como esses componentes estão diretamente envolvidos com o controle de funções operacionais de infraestruturas, o comprometimento de sistemas SCADA pode ser considerado crítico por empresas e governos, especialmente no caso de sistemas SCADA controladores de infraestruturas essenciais.

Por outro lado, os recursos cibernéticos podem também performar desdobramentos nas dimensões físicas sem envolver ações coercitivas, como a utilização da informação para induzir determinados comportamentos e pautar as concepções ideológicas das pessoas. Ora, uma vez que a informação criada e difundida por meio do ciberespaço alcança pessoas em todas as regiões do globo, a utilização da informação e o direcionamento dela para públicos pré-determinados, especialmente através das mídias sociais, pode contribuir para a conformação de uma opinião pública que defenda ideologias ou agendas que estejam alinhadas aos interesses do Estado arquiteto

[8] Segundo a Microsoft (2012, s/p, tradução própria) "A injeção de SQL é um ataque no qual um código malicioso é inserido em strings que posteriormente são passadas para uma instância do SQL Server para análise e execução. Qualquer procedimento que construa instruções SQL deve ser revisado para vulnerabilidades de injeção porque o SQL Server executará todas as consultas sintaticamente válidas que receber. Mesmo dados parametrizados podem ser manipulados por um invasor habilidoso e determinado".

[9] Nas palavras de Clarke e Knake (2012), "uma bomba-lógica, na sua forma mais básica, é simplesmente um apagador: ela apaga todos os softwares em um computador, deixando-o como se fosse uma inútil caixa de metal. Bombas-lógicas mais avançadas poderiam primeiramente fazer com que o hardware fizesse algo para se autoprejudicar, como produzir um pico de energia que torrasse os circuitos dos transformadores, ou fazer com que os controles de um avião o colocassem em posição de mergulho, para em seguida apagar tudo, inclusive a si mesma."

da ação. Alguns exemplos de recursos com esse intuito são técnicas de operações psicológicas, difusão de desinformação e propaganda política (GILES, 2016a).

Nesse sentido, os recursos de poder cibernético, no conceito *soft*, servem aos auspícios de um Estado que objetive, por exemplo, a mudança da composição política do governo que dirige uma determinada nação ou a desestabilização das instituições de Estado e de governo através de um processo político interno degradante (GHERNAOUTI, 2013).

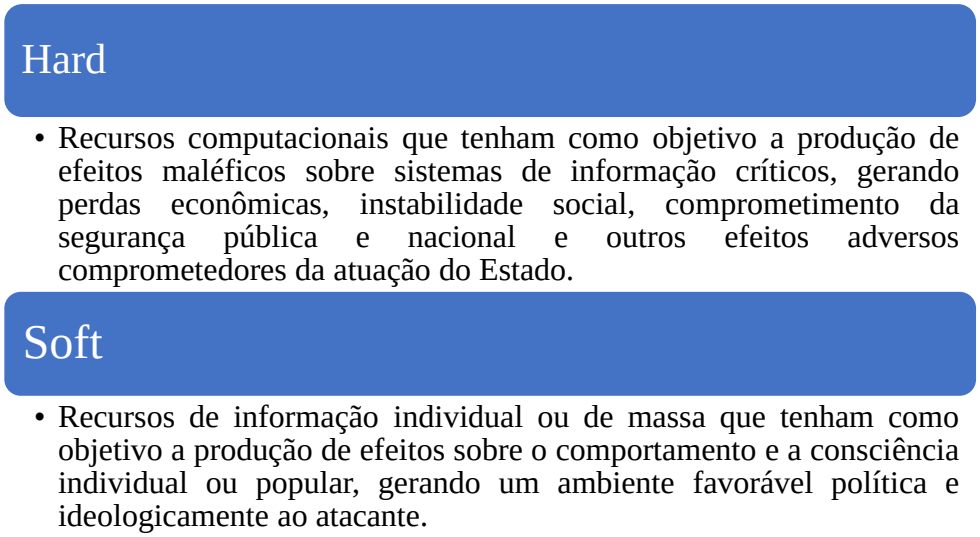
Nessa perspectiva, as mídias sociais e outros meios de comunicação na internet, servem como recursos *soft* de poder cibernético, uma vez que a participação de um número cada vez maior de pessoas nesses ambientes digitais torna-os importantes difusores de propaganda política, seja diretamente ou indiretamente (AYRES PINTO; MORAES, 2020).

Para Ayres Pinto e Moraes (2020) a estrutura e o algoritmo das redes sociais operam no sentido de limitar o debate político, de promover uma falsa percepção de participação ativa e decisória do que se visualiza e do que se deseja no meio digital. Tal mecanismo também expõe as pessoas a informações que, em certos casos, não possuem respaldo na realidade dos fatos. Assim sendo, as redes sociais, além de funcionarem muito bem para a propagação de ideais políticos, podem ser utilizadas em operações psicológicas que busquem influenciar a percepção das pessoas e atraí-las para determinadas narrativas. Ações nesse sentido foram reveladas e amplamente divulgadas no escândalo da Cambridge Analytica (CONFESSORE, 2018).

Van Niekerk e Maharaj (2012) demonstram como as mídias sociais, tiveram papéis de relevância em muitas situações de conturbações políticas, sociais e militares atualmente. Nessa perspectiva, os autores pontuam que as mídias sociais podem ser utilizadas, por exemplo, para fins de guerra de informação, operações de influência e operações psicológicas, à serviço de Estados e outras organizações.

Nessa perspectiva e após o exame dos diversos recursos que existem no ciberespaço que podem ser utilizados e manipulados para finalidades de projeção de poder dos Estados, a Figura 4 sintetiza o entendimento de o que são recursos cibernéticos, de acordo com as vertentes *hard* e *soft*, para os fins desse trabalho.

Figura 4 – Recursos de poder cibernético



Fonte: elaboração própria com base nas leituras de Nye (2010), Giles (2016a), Ghernaouti (2013), Ayres Pinto e Moraes (2020) e Van Niekerk e Maharaj (2019).

Após o escrutínio dos diferentes recursos de poder cibernéticos e a sua conceituação em termos de *hard* e *soft power*, o item seguinte trata da questão da guerra e busca mostrar como a utilização dos recursos de poder cibernético, em termos de guerra cibernética e de informação, encontra respaldo nos âmbitos estratégico, tático e operacional das operações militares.

2.3 A GUERRA MODERNA E A RELAÇÃO COM A TECNOLOGIA DO CIBERESPAÇO

A guerra é uma expressão utilizada recorrentemente para tratar de conflitos em que há a aplicação da violência física continuada entre dois ou mais atores internacionais, ainda que o direito internacional somente reconheça oficialmente a ocorrência de guerras nos atos conflitivos armados entre Estados. Entretanto, a bibliografia acadêmica das áreas que estudam a temática do conflito nas relações internacionais, costumam se referir ao termo guerra de forma mais ampla, abrangendo diferentes categorias de atores internacionais e, além disso, inclui formas de conflito que não apenas as que envolvem a ocorrência de violência física.

Conforme será trabalhado no Capítulo 3, os conceitos estratégicos, táticos e operacionais das guerras no século XXI, de acordo com o que é concebido pela Rússia, estão atrelados às capacidades ofensivas dos recursos cibernéticos, em diferentes frentes de ação. Desse modo, os

recursos cibernéticos representam um papel de relevância na condução da guerra pelos russos, servindo como um artificio de importância para o cumprimento dos objetivos de política externa e defesa nacional do país.

Desse modo, a presente seção procede ao exame da temática a partir de uma abordagem teórica que considera o caráter evolutivo da guerra, de modo a permitir uma aproximação da concepção geral dos desdobramentos da guerra - em termos atuais - com a compreensão russa sobre os processos conflitivos do século XXI, bem como, da posição de suas capacidades ofensivas nesse contexto. A guerra de informação é inserida no final dessa explanação, de modo a apresentar como os elementos de poder cibernético *hard* e *soft* são empregados no âmbito da guerra.

2.3.1 O caráter geracional das guerras

O tema do conflito violento entre comunidades humanas já era tratado muito antes do surgimento dos primeiros Estados nacionais, podendo ser citado os escritos de Sun Tzu em A Arte da Guerra, que data de cerca de 320 a 400 anos A.C. A validade das descrições feitas por Sun Tzu sobre estratégias e táticas de guerra permaneceram por muito tempo quase inalteradas, sendo que mesmo nos tempos atuais as considerações feitas pelo estrategista chinês continuam relevantes no campo estratégico. Outro nome importante nesse entendimento é o do general prussiano Carl von Clausewitz, em seu conhecido tratado Da Guerra, em que foram feitas considerações sobre as dinâmicas das guerras em nível estratégico e operacional, mas o autor também se preocupou em tratar da matéria de maneira mais holística, isto é, procurou analisar a guerra conforme a sua complexidade intrínseca, ao considerar conjuntamente as diferentes variáveis que influem nos conflitos. Foi também Clausewitz que sintetizou o objetivo de caráter político da guerra em sua famosa frase “A guerra é, portanto, um ato de força para obrigar nosso inimigo a fazer a nossa vontade” (CLAUSEWITZ, 2007).

Contudo, em tempos recentes, alguns autores passaram a tratar o estudo da guerra por meio de uma abordagem evolutiva, observando as principais diferenças nos níveis estratégicos, táticos e operacionais das guerras ao longo do tempo. Nesse sentido, Lind et al (1989) faz uma teorização sobre o caráter evolutivo das guerras, em termos qualitativos, dissertando que podem ser relacionadas três gerações de guerra e, em seguida, discute sobre as características de uma quarta geração. Cabe ressaltar que, por outro lado, o autor frisa que a fundamentação das guerras em

termos geracionais não se trata de uma verificação necessariamente cronológica, tendo em vista que mesmo nas guerras atuais marcos conceituais, estratégicos e táticos de outras gerações permanecem sendo utilizados pelas forças nacionais regulares. Para Lind et al (1989), as forças que alteram a forma de fazer guerra e que, portanto, dão razão a uma segmentação geracional dos tipos de guerra, são a tecnologia e as ideias.

Segundo Reed (2008), as guerras de primeira geração podem ser particularmente caracterizadas por batalhas que envolviam linhas e colunas de soldados, portando mosquetes, como uma tática de potencializar o poder humano empregado, como meio principal de combate. Ademais, essas guerras ocorreram entre Estados e possuíam finalidades políticas primárias, sendo que as estratégias e táticas desse tipo de guerra são encontradas, por exemplo, na obra de Clausewitz (2007).

As guerras de segunda geração foram profundamente influenciadas pelas mais novas tecnologias desenvolvidas a partir da segunda Revolução Industrial, ocorrida entre o final do século XIX e início do XX. As novas técnicas de produção resultaram na introdução de novos recursos para a execução dos conflitos, com a infantaria equipada com armas com maior poder de fogo, como os rifles e as metralhadoras e o aumento de capacidade de fogo indireto dos instrumentos de artilharia, desse modo, o poder de fogo passava a superar o poder humano para o desfecho vitorioso do conflito. Tais soluções tecnológicas imprimiram novas dinâmicas às batalhas, demandando mudanças de abordagem por parte dos estrategistas militares, sendo uma das mais significantes a adoção da guerra de trincheiras como tática marcante na Primeira Guerra Mundial (1914-1918) (REED, 2008).

Por sua vez, as guerras de terceira geração - ainda mantendo a primazia do conflito entre Estados nacionais – aproveitaram-se do aprimoramento tecnológico dos recursos desenvolvidos para acrescentar um novo elemento às dinâmicas dos conflitos, a realização da guerra de forma conjunta em diferentes domínios: terra, ar, mar e, inclusive, ciberespaço. Ainda que os primeiros indícios de uma nova evolução na forma de fazer guerra tenham surgido ao final da Primeira Guerra Mundial (1914-1918), foram os alemães, em eventos antecedentes e durante a Segunda Guerra Mundial (19139-1945), que aprimoraram o ambiente operacional da guerra por meio da *blitzkrieg*. A partir de uma concepção tática fundamentada mais em capacidade de manobra e menos em atrito, os alemães perceberam que poderiam contornar as forças inimigas e incapacitá-las através do

colapso de suas linhas de suporte, em vez de realizar o confronto direto (LIND et al, 1989; REED, 2008).

A terceira geração permanece sendo o principal marco conceitual na forma de praticar a guerra presente nas forças armadas no mundo. Já a quarta geração marca uma importante mudança conceitual: o envolvimento direto de atores não-estatais no conflito. Lind et al (1989), observando o desenvolvimento das guerras de quarta geração, resume as quatro ideias centrais que as fundamentam:

> A primeira são as ordens da missão. Cada mudança geracional foi marcada por uma maior dispersão no campo de batalha. É provável que o campo de batalha da quarta geração inclua toda a sociedade inimiga. Essa dispersão, juntamente com o que parece ser de maior importância para ações de grupos muito pequenos de combatentes, exigirá até o nível mais baixo para operar de maneira flexível com base na intenção do comandante. O segundo é a dependência decrescente da logística centralizada. A dispersão, juntamente com o aumento do valor colocado no tempo, exigirá um alto grau de habilidade de sobrevivência em relação ao terreno e ao inimigo. Terceiro, mais ênfase na manobra. Massa, de homens ou poder de fogo, não será mais um fator avassalador. De fato, a massa pode se tornar uma desvantagem, pois será fácil visualizá-la. Forças pequenas, altamente manobráveis e ágeis tenderão a dominar. Quarto é o objetivo de derrubar o inimigo internamente, em vez de destruí-lo fisicamente. As metas incluirão coisas como o apoio da população à guerra e a cultura do inimigo. A identificação correta dos centros de gravidade estratégicos inimigos será altamente importante (LIND et al, 1989, s/p, tradução própria).

Já Reed (2008) faz uma observação mais geral do ambiente conceitual estratégico e tático das guerras de quarta geração, dissertando que:

> As características da guerra de quarta geração lhe conferem uma vantagem dialética sobre a guerra de terceira geração e permitem que forças quantitativa e qualitativamente inferiores conquistem forças superiores de tamanho ou armamento. Ele usa estratégias e táticas assimétricas, aplicadas por longos períodos de tempo, para desviar o foco da destruição das forças militares convencionais superiores de um inimigo - as quais ele não pode derrotar - e, em vez disso, a derrota da vontade política inimiga de lutar. Combina a força política de um oponente contra a força política do outro (REED, 2008, p. 688, tradução própria).

Conforme explica Reed (2008), a alteração substancial está na disputa entre um ator com poder de fogo superior e outro com um poder de fogo inferior, onde o segundo pode vencer a guerra por meio da utilização de recursos assimétricos, como, por exemplo, a vontade política para lutar. Ao citar Hammes (2004), Reed (2008) disserta que as estratégias e táticas das guerras de quarta geração assemelham-se em muito com uma forma evoluída de guerra de insurgência.

O sucesso de atores não-estatais em confrontar inimigos com poder de fogo substancialmente superior por meio da adoção de estratégias e táticas assimétricas – sendo verificáveis variações e adaptações nesses métodos - ocorreram em vários acontecimentos, como

os vietcongues contra os EUA e tropas sul-vietnamitas na Guerra do Vietnã (1955-1975), os afegãos contra os soviéticos na Guerra do Afeganistão (1979-1989) e o grupo terrorista Al Qaeda novamente contra os estadunidenses nos eventos que se seguiram ao 11 de setembro de 2001 e das operações da campanha da Guerra ao Terror (REED, 2008).

2.3.2 Guerras no século XXI: Guerras de quinta geração e guerra de informação

Enquanto para Lind et al (1989) os principais impulsionadores de mudanças nas características das guerras ao longo do tempo são a tecnologia e as ideias, Hammes (2004) vai além e defende que as alterações na forma de fazer guerra decorrem de mudanças nas áreas políticas, sociais, econômicas e tecnológicas das comunidades humanas. Nessa concepção, pode ser entendido o novo conceito de guerra - ou o que Reed (2008) chama de guerra de quinta geração.

Reed (2008) ao estabelecer uma abordagem multidimensional para realizar a análise do caráter geracional das guerras, relaciona quatro eixos evolutivos: domínios de conflito, natureza dos adversários, natureza dos objetivos (formas de derrotar o inimigo) e natureza das forças. Ao utilizar esses quatros eixos, é possível caracterizar as guerras de quinta geração, sob a concepção teórica do autor. Em primeiro lugar, as guerras de quinta geração podem ser destacadas pelo desenvolvimento de práticas conflitivas nos domínios geográficos (terra, ar e água), no domínio da informação, no domínio cognitivo e no espaço social – e político. Reed (2008) define esses domínios da seguinte forma:

> Domínio físico: O domínio tradicional da guerra, onde uma força é movida através do tempo e do espaço. Ele abrange os domínios terrestres, marítimos, aéreos e espaciais tradicionais, onde as forças militares executam operações e onde a maioria das guerras convencionais é conduzida.
> Domínio da informação: O domínio em que as informações são criadas, manipuladas e compartilhadas. Abrange o domínio cibernético.
> Domínio cognitivo: O domínio em que residem intenção, doutrina, tática, técnicas e procedimentos. É o domínio em que conceitos decisivos emergem.
> Domínio Social: Compreende os elementos necessários de qualquer comunidade humana. É onde os humanos interagem, trocam informações, formam consciência e entendimento compartilhados e tomam decisões colaborativas. É também o domínio da cultura, religião, valores, atitudes e crenças, e onde as decisões políticas relacionadas à "vontade da comunidade" são tomadas (REED, 2008, p. 692, tradução própria).

No que tange à natureza dos adversários, as guerras de quinta geração expandem a quantidade de atores capacitados em fazer guerra, em comparação com a quarta geração. Nesse caso, os efeitos da globalização e da era da informação foram primordiais para o surgimento de

novas redes e organizações de indivíduos com interesses próprios e meios de perpetrar ações ofensivas, até mesmo contra Estados. Haja vista que o acesso à recursos econômicos, financeiros, bélicos e de informação foi facilitado a entidades civis com capacidades relativas significativas passaram a tomar novos espaços nas relações internacionais (REED, 2008).

Em relação às formas de atingir os objetivos, os mecanismos de derrotar o inimigo, o autor coloca que as guerras de quinta geração utilizam especialmente a tática da implosão, isto é, a derrota do inimigo por meio da neutralização ou destruição de seus processos internos, que dão origem, razão e capacidade para a sua operação. Desse modo, podem ser citados processos como a construção de alianças, a formação de lideranças, a divulgação de propaganda ideológica e política, os meios de financiamento, as comunicações, os métodos de planejamento, dentre outras questões (REED, 2008).

No que concerne a natureza da força nas guerras de quinta geração, Reed (2008) disserta que as possibilidades também são expandidas, podendo haver o uso tanto de forças cinéticas quanto não cinéticas, tendo em vista a existência de capacidades em ambos os métodos para o cumprimento do objetivo político da guerra, qual seja, o definido por Clausewitz (2007), dado que os recursos atuais de poder, mesmo os não cinéticos, possuem capacidade de constranger o inimigo, em graus relativos.

Liang e Xiangsui (1999) trazem a discussão sobre a nova forma de fazer guerra numa lógica similar ao texto de Reed (2008), no sentido de identificar que existem métodos cinéticos e não cinéticos a disposição dos atores internacionais que podem ser utilizados para implementar a guerra, sem alterar os seus objetivos e o sucesso para alcançar seus fins. Os autores adotam uma visão de que o uso individual de meios letais para a resolução de conflitos se tornou algo excessivamente custoso e problemático nos tempos recentes, haja vista o dispêndio de montantes cada vez mais altos de recursos econômicos para o desenvolvimento e aprimoramento de armamentos convencionais, com uma tendência de implementação de tecnologia de ponta em muitas das armas, requisitando investimentos elevados. Além disso, o desenvolvimento de novos armamentos convencionais potencializa o surgimento de uma corrida armamentista (LIANG; XIANGSUI, 1999), como uma consequência do Dilema de Segurança.

Nesse sentido, Liang e Xiangsui discutem sobre o ‘novo conceito de armas’, que difere em praticamente todas as características aos meios de emprego da força tradicionais, quais sejam, os meios militares. Liang e Xiangsui (1999) ressaltam que o novo conceito de armas não significa o

simplesmente incremento tecnológico de armamentos convencionais, mas que faz parte de um "processo de criação de armas que são intimamente ligadas às vidas de pessoas comuns...[...] Acreditamos que algumas pessoas acordarão pela manhã para descobrir com surpresa que algumas coisas então inofensivas começaram a ter características ofensivas e letais" (LIANG; XIANGSUI, 1999, p. 26, tradução própria).

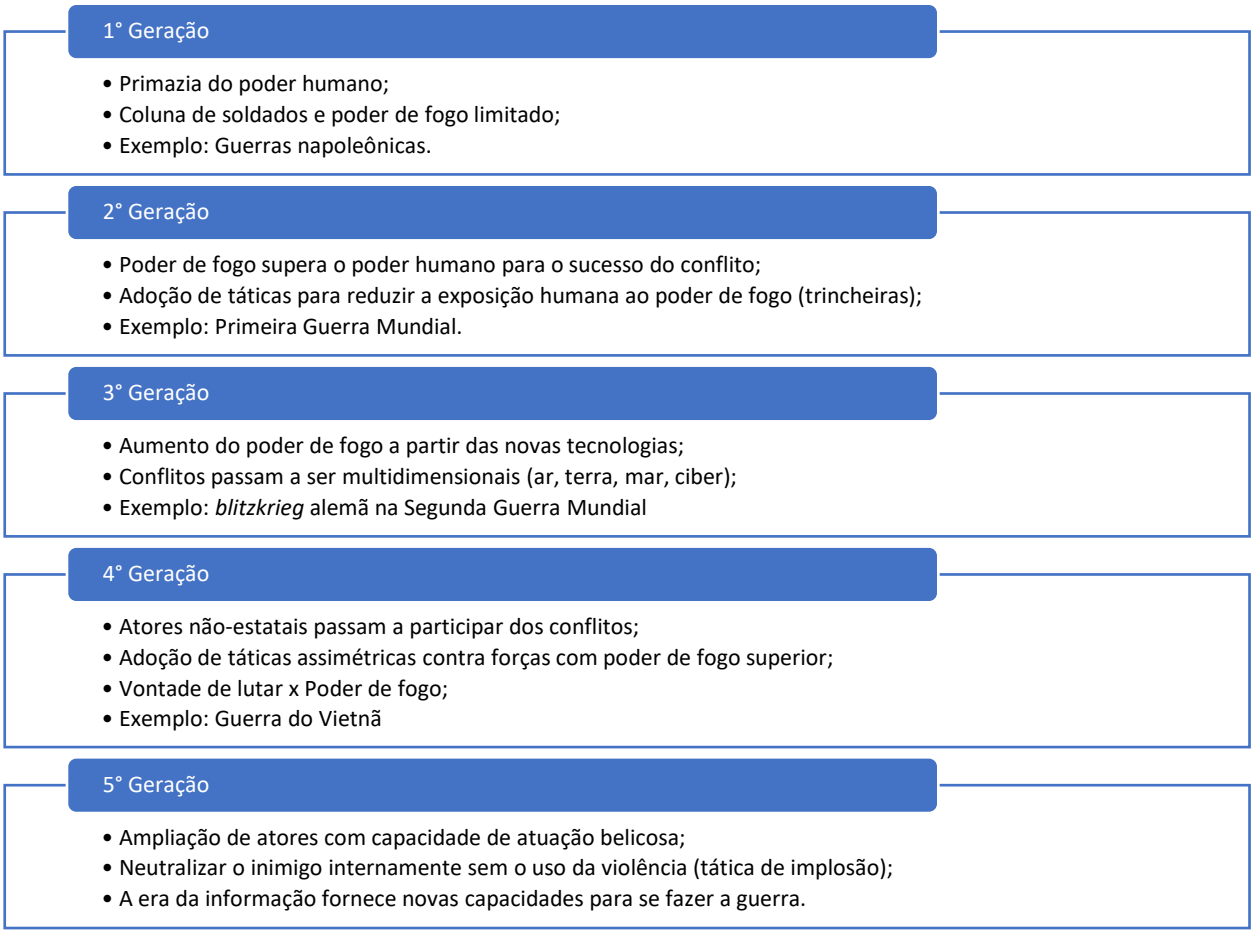
Para os autores, o progresso tecnológico oportunizou a utilização de novos recursos e métodos para atingir o centro de gravidade do adversário, sem imprimir consequências negativas em outras estruturas ou indivíduos, assim há uma mudança de perspectiva de que a melhor maneira de se obter a vitória na guerra não é necessariamente matar, mas sim controlar o inimigo. As novas soluções no campo militar, por exemplo, como o desenvolvimento de armas de precisão, diminuíram significativamente a perda de vidas humanas em conflitos ao redor do mundo nos últimos tempos (LIANG; XIANGSUI, 1999).

Dessa forma, as armas estão sendo desenvolvidas em uma direção 'mais gentil', no lugar da 'de mais força' que era a tendência passada, vide o exemplo das armas de destruição em massa. A partir da perspectiva de que as armas mais gentis derivam do novo conceito de armas, os autores indicam que as armas de informação são o exemplo mais notável de armas mais gentis, haja vista que os recursos de *hard e soft power* próprios do meio cibernético possuem como focos a paralisação e desestabilização do inimigo, e não a perda de vidas humanas (LIANG; XIANGSUI, 1999).

Como pode ser notado nas leituras de Reed (2008) e Liang e Xiangsui (1999), o elemento cibernético detém uma posição de relevância no âmbito estratégico e tático das guerras no contexto do século XXI, uma vez que o domínio cibernético aparece como um dos campos de batalha e, por sua vez, os recursos cibernéticos surgem como novas armas.

Por fim, a Figura 5 consolida todo o exposto neste subcapítulo, sintetizando as principais características das guerras de cada geração.

Figura 5 – Principais características de cada geração



Fonte: Elaboração própria com base nas leituras de Lind *et al* (1989), Reed (2008), Hammes (2004) e Liang e Xiangsui (1999).

Nesse âmbito, a guerra de informação ou guerra informacional é a tipologia utilizada para se referir aos conflitos que se utilizam, dentre outros, do ciberespaço e de seus recursos de forma ofensiva. Para Kuehl (2002, p. 36, tradução própria) a guerra de informação pode ser definida como "operações de informação conduzidas durante tempos de crise ou conflito para alcançar ou promover objetivos específicos sobre um adversário ou adversários específicos". Por sua vez, o autor define operações de informação como "ações tomadas para afetar a informação e os sistemas de informação do adversário enquanto defende as próprias informações e sistemas de informação" (KUEHL, 2002, p. 36, tradução própria).

Ainda de acordo, ambos os termos podem também ser entendidos como:

> a luta para controlar e explorar o ambiente de informação, uma luta que se estende por todo o espectro do conflito da "paz" à "guerra" e envolve virtualmente todas as agências e instrumentos de poder do governo (KUEHL, 2002, p. 37, tradução própria)

Desse modo é possível relacionar a concepção da guerra de informação com as características das guerras de quinta geração como descrito por Reed (2008), isto é, o foco em incapacitar e desmobilizar o adversário por meio da realização de ações que impactem nos domínios da informação, cognitivo e social. Outra característica relevante colocada por Kuehl (2002) é no que se refere ao contexto temporal da guerra de informação, uma vez que ela pode estar sempre presente, dos tempos de paz até o de guerra.

É necessário ainda segregar as formas da guerra de informação, tendo em vista a exploração da maneira como os elementos de poder cibernético nas dimensões hard e soft são utilizados dentro desse conceito. O Departamento de Defesa dos EUA (DoD) compreende que a guerra de informação é constituída por cinco categorias de capacidades: (1) *Psychological Operations* (PsyOps), (2) *Military Deception*, (3) *Operational Security*, (4) *Computer Network Operations* (CNO), and (5) Electronic Warfare (CRS, 2009).

Para os fins deste trabalho, as PsyOps e as CNO são as categorias que mais interessam para examinar as ações da Rússia no âmbito cibernético. O DoD define as PsyOps como sendo:

> operações planejadas para transmitir informações selecionadas para públicos estrangeiros direcionados para influenciar suas emoções, motivos, raciocínio objetivo e, em última análise, o comportamento de governos, organizações, grupos e indivíduos estrangeiros. [...] Os produtos criados para PSYOP devem ser baseados em conhecimento profundo dos processos de tomada de decisão do público-alvo. Usando esse conhecimento, os produtos PSYOPS devem ser produzidos rapidamente e disseminados diretamente para públicos-alvo em toda a área de operações (CRS, 2009, p. 30, tradução própria)

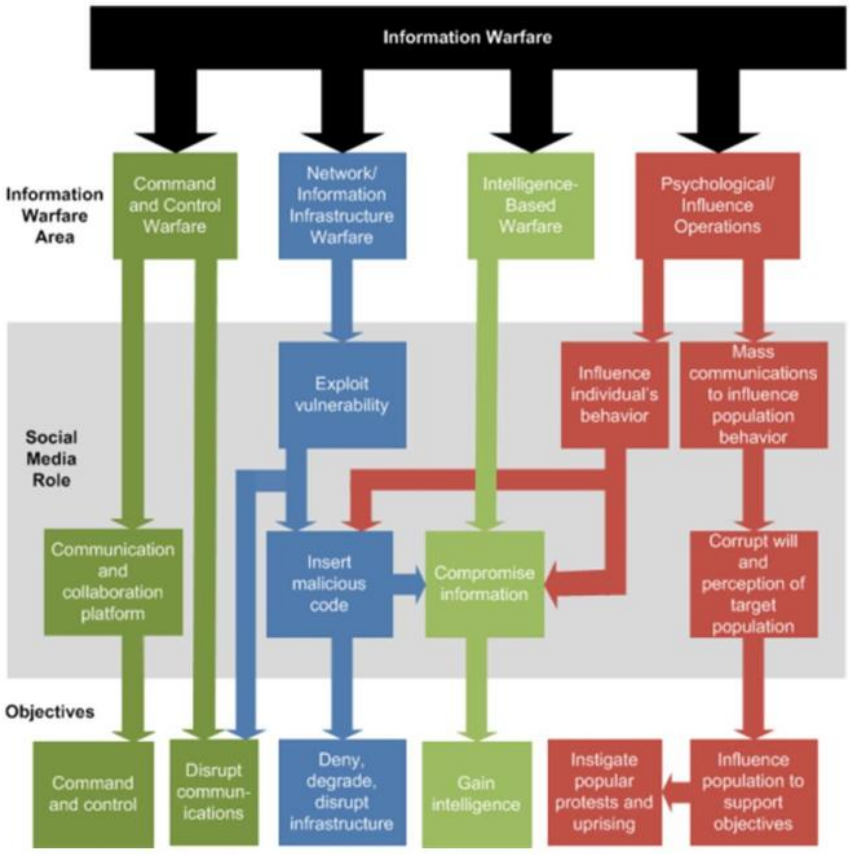
De outro modo, as CNO incluem:

> (1) atacar e interromper redes de computadores inimigas; (2) defender nossos próprios sistemas de informação militar; e (3) explorar redes de computadores inimigas por meio da coleta de inteligência, geralmente feita por meio do uso de código de computador e aplicativos de computador (CRS, 2009, p. 30, tradução própria).

As PsyOps estão relacionadas especialmente com as mídias sociais, as quais estão amplamente presentes na Internet. Outra forma de compreender as PsyOps é a utilização do termo ‘desinformação’ ou ‘desinformação digital’ para se referir as operações realizadas no meio virtual. De acordo com a UNESCO (2018, s/p, tradução própria), desinformação são “informações falsas criadas deliberadamente para prejudicar uma pessoa, grupo social, organização ou país”. O termo também é popularmente conhecido como “*fake news*”.

Abaixo, a Figura 6 apresenta um esquema que expõe as atribuições das mídias sociais como recursos de poder cibernético, no âmbito de uma estratégia de guerra de informação.

Figura 6 – Atribuições das mídias sociais no âmbito da guerra de informação



Fonte: Van Niekerk e Maharaj (2012, s/p).

Conforme pode ser visto na Figura 6, os autores separaram a guerra de informação em cinco áreas diferentes e, para cada, estabeleceram quais usos são feitos das redes sociais. Dessa forma, encontram-se diversas funcionalidades, que variam conforme os objetivos de cada área, funcionando como uma plataforma de comunicação e colaboração, para exploração de vulnerabilidades em infraestruturas críticas; inserção de informações comprometedoras; influência no comportamento de indivíduos ou de população; e desvirtuamento da percepção e dos propósitos de uma população-alvo.

As CNO, por outro lado, apesar também servirem para as atividades de desinformação e PsyOps, tem como ponto central operações ofensivas com o objetivo de “interromper, negar,

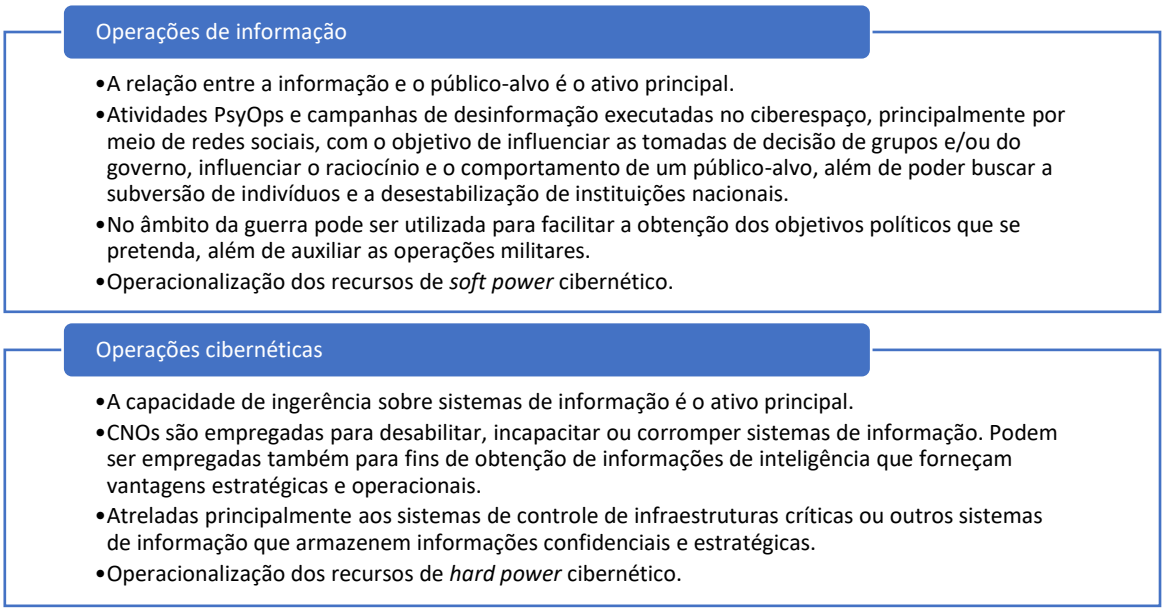
degradar ou destruir informações residentes em computadores e redes de computadores ou os próprios computadores e redes" (KUEHL, 2002, p. 44, tradução própria). Podem também ser operações de exploração dos sistemas de informação do adversário para:

> coleta de inteligência que obtêm informações armazenadas em arquivos de sistemas de informação automatizados (AIS) e obtêm informações sobre vulnerabilidades potenciais, ou acessam informações críticas armazenadas em AIS estrangeiros que poderiam ser usadas em benefício de operações amigáveis (KUEHL, 2002, p. 44, tradução própria).

Para fins didáticos e de facilitação da apresentação das características das ações russas, a partir daqui as PsyOps, desinformação digital e outros termos que compreendam esse escopo de conceitos serão chamados somente de operações de informação (InfoOps), uma vez que o aspecto central dessas operações é a forma com que a informação é manipulada, transmitida e assimilada pelo público-alvo. De outro modo, as CNOs, compreendendo a divisão as entre atividades ofensivas e de exploração serão chamadas somente de operações cibernéticas (CyberOps), dado que, nesse caso, a dimensão principal são as ações coercitivas relacionadas aos sistemas de informação do adversário.

A Figura 7 sintetiza o entendimento do que são InfoOps e CyberOps no contexto do objetivo desse trabalho, compreendendo-se a sua execução no âmbito da guerra de informação, além da relação entre essas formas de operação e os recursos de poder cibernético discutidos no item 2.2.3.

Figura 7 – Operações de informação e operações cibernéticas



Fonte: Elaborado com base nas leituras de Kuehl (2002), CRS (2009), Hatch (2019) e Lilly e Cheravitch (2020).

2.4 CONCLUSÕES PARCIAIS

Este capítulo tratou do arcabouço teórico que fundamenta este trabalho. Foram trabalhados três eixos principais: a compreensão do poder cibernético de acordo com as teorias neorealista e construtivista das relações internacionais, a securitização e instrumentalização do ciberespaço pelos Estados (recursos de poder cibernético nas dimensões *hard* e *soft*) e, por fim, a relação entre a tecnologia e a guerra, abordando-se os conceitos de guerra de quinta geração e guerra de informação.

No que se refere ao poder cibernético, inicialmente foi realizada uma breve contextualização das teorias de poder na Ciência Política e, em seguida, nas Relações Internacionais. Logo depois, foi proposta uma leitura do poder cibernético sob a ótica das teorias neorealista e construtivista, possibilitando-se a obtenção da compreensão de um caráter dual que o poder cibernético pode assumir: pelo lado neorealista, uma abordagem do ciberespaço como um novo ambiente para o desenvolvimento de capacidades de poder coercitivo; enquanto pelo lado construtivista, os elementos informacionais operam como uma forma de projeção e modelagem de

ideologias, percepções e narrativas, alcançando tanto o nível dos tomadores de decisão quanto da população em geral.

Esse aspecto dual do poder cibernético é, por sua vez, conectado com a realidade que se impõe, isto é, como o ciberespaço, por meio das soluções de TIC, está cada vez mais presente no cotidiano, seja na forma de *softwares* que automatizam e controlam processos de infraestruturas civis e militares essenciais para a manutenção da ordem social, seja na vida de cada cidadão, por meio das mídias e redes sociais. Desse modo surgem os recursos de poder cibernéticos, computacionais (*hard*) e informacionais (*soft*), produzindo efeitos internamente e externamente ao conteúdo do ciberespaço.

Por fim, a introdução da guerra nesse arcabouço é importante para que seja possível assimilar como esses recursos de poder cibernético, em termos de estratégias e táticas, podem ser empregados por atores internacionais para o alcance de objetivos políticos. Dessa maneira, a observação do ciberespaço como uma dimensão dos conflitos ainda no âmbito das guerras de terceira geração e, em seguida, a conjectura do papel que os recursos cibernéticos assumem como centrais na concepção da guerra moderna, permitem entender o caráter multifatorial que os recursos cibernéticos podem ser compreendidos em termos bélicos, isto é, como parte integrante e auxiliadora de um esforço militar complexo e como elemento primário de uma estratégia de neutralização do inimigo sem o recurso à força. Por fim, a apresentação do conceito de guerra de informação e a sistematização das CyberOps e InfoOps auxiliam nos demais capítulos a compreender como os recursos cibernéticos são de fato empregados pela Rússia.

3 A POLÍTICA ESTRATÉGICA DA RÚSSIA NO SÉCULO XXI

Este capítulo procura analisar a política estratégica da Rússia no século XXI, compreendendo o período das presidências de Vladimir Putin (2000-2008; 2012-atual) e Dmitry Medvedev (2008-2012). Para tanto, são considerados os contextos do ambiente nacional e política interna da Rússia desde o fim da URSS em 1991, inclusive com relação às circunstâncias socioeconômicas do país. Em seguida, a política externa do país é colocada em perspectiva, destacando-se os seus fundamentos conceituais e a relação da Rússia com o Ocidente, particularmente com os EUA e a OTAN.

Logo após, a política de segurança nacional e defesa é analisada, tomando como base os principais apontamentos obtidos pelo exame da política externa russa. Desse modo, procura-se estabelecer a relação entre esses dois escopos pertencentes à política estratégica do país, como maneira de fundamentar a posterior compreensão da função dos elementos cibernéticos na perseguição dos principais objetivos da Rússia no que tange às suas relações internacionais.

Por fim, o componente cibernético é inserido como um instrumento de defesa nacional nesse contexto, sobretudo no que se refere à doutrina militar-estratégica russa, abordada na análise da política de segurança nacional de defesa. Nessa sequência, é apresentado e explorado o modelo de guerra híbrida, considerado o conceito operacional de guerra moderna da Rússia, no qual os recursos cibernéticos possuem participação essencial.

3.1 POLÍTICA INTERNA NA RÚSSIA PÓS-SOVIÉTICA

A Rússia do século XXI é um produto direto da dissolução da URSS. Como principal herdeira política do império soviético, o país se viu também mergulhado no caos político, social e econômico que assolou as ex-repúblicas soviéticas em especial durante os anos 90.

A transição de um regime autoritário para um regime – em certa medida - liberal democrático e de uma economia socialista planificada para uma economia capitalista de mercado, atingiu amplamente toda a sociedade e institucionalidade russas. Portanto, é importante analisar como a Rússia se reorganizou internamente como Estado e, de que maneira, essa reorganização a partir dos anos 2000 se traduziu em termos de uma política externa mais ambiciosa e assertiva.

3.1.1 Período Yeltsin (1991-1999)

Em 1991, nos momentos finais da dissolução da URSS, Boris Yeltsin assume como presidente da recém independente Federação Russa. O seu mandato – que durou até 1999 quando renunciou, dando lugar ao seu primeiro-ministro Vladimir Putin – foi marcado por turbulências políticas internas e por uma economia totalmente enfraquecida. No âmbito econômico, uma de suas primeiras medidas foi a realização da privatização das propriedades do Estado, passando assim importantes companhias públicas para a iniciativa privada, como as indústrias produtoras de *commodities* energéticas – até hoje o principal produto da matriz econômica da Rússia (SEGRILLO, 2012; OEC, 2020).

Entretanto, o modo como foram conduzidas as privatizações criou uma comunidade de oligarcas russos, pessoas que possuíam cargos de alto escalão nas companhias soviéticas e que, portanto, detinham maiores condições financeiras e influência política para comprarem as empresas russas, que foram vendidas por preços muito abaixo dos de mercado. Dessa maneira, a repentina criação dessa elite oligárquica tornou ainda mais instável o novo ambiente político, que passou também a ter pressões vindas de representações que defendiam o retorno ao sistema soviético; de grupos liberais que buscavam o desenvolvimento na Rússia de um Estado nos moldes das democracias ocidentais e de organizações nacionalistas que defendiam o resgate de uma memória gloriosa da Rússia imperial (SEGRILLO, 2012).

Tais conturbações políticas tiveram como um de seus efeitos práticos os confrontos violentos em Moscou, no segundo semestre de 1993, conhecido como a crise constitucional da Rússia. A luta de poder entre o Executivo e do Legislativo russo causaram divisões entre Yeltsin e o parlamento, com as tensões crescendo desde o final do ano de 1992 e a realização de medidas de ambos os lados para deslegitimar o contrário. Então, em setembro de 1993, Yeltsin anunciou a dissolução do parlamento russo, afirmando que iria legislar por decreto até a realização de novas eleições. Tal ação foi vista pelo legislativo como uma afronta de Yeltsin à constituição, como reação o parlamento o destituiu da presidência, nomeando o então vice-presidente em seu lugar (SHARLET, 2013).

O ambiente econômico extremamente fragilizado, acusações de corrupção e a insatisfação popular geral com a situação do país levaram também a protestos nas ruas de Moscou nesse período. Em meio aos confrontos na rua, Yeltsin, contando com o apoio das forças armadas, cercou

o parlamento com tanques e ordenou o bombardeamento do prédio, além da prisão de quem estava no interior do edifício (SHARLET, 2013).

Em 1994 a ação de movimentos separatistas e a reinvindicação de autonomia na república da Chechênia, uma subdivisão administrativa da federação localizada na região do Cáucaso, foram respondidos com a invasão do território pelo exército russo para a manutenção da união russa (HART; HESS, 2001).

A deterioração da situação na região e a repercussão na opinião pública no restante da Rússia e fora do país pressionou Yeltsin a retirar as tropas da Chechênia em 1996, ação que também teve consequências negativas sobre o governo, pois demonstrou a incapacidade de Yeltsin em estabelecer a união do território russo e refletiu a imagem da fragilidade em que se encontravam as forças armadas do país, com graves problemas na formação da infantaria, no sucateamento dos equipamentos militares, no planejamento e nas táticas de conflito (HART; HESS, 2001).

Depois de anos enfrentando graves problemas econômicos, a Rússia viu um aprofundamento da crise em 1998, quando um reflexo da crise financeira ocorrida nas bolsas de valores de países asiáticos atingiu o sistema financeiro russo. A fuga de capitais do país que se seguiu e a queda dos preços do petróleo resultaram em uma grande desvalorização do rublo, o que agravou ainda mais a já debilitada economia, com níveis altos de inflação. Sem divisas para cumprir com os pagamentos da dívida externa, a Rússia declarou moratória, tendo de recorrer ao Fundo Monetário Internacional (FMI) em busca de empréstimos para reestruturar a sua dívida com os credores internacionais (SLAY, 1999).

A seguir são exibidos e analisados alguns indicadores macroeconômicos da Rússia durante o governo Yeltsin, de forma a transmitir a gravidade dos problemas enfrentados pelo país nos anos 90, bem como os reflexos sobre a população russa. Desse modo, o Gráfico 2 apresenta os dados do crescimento do Produto Interno Bruto (PIB) da Rússia entre 1991 e 1999.

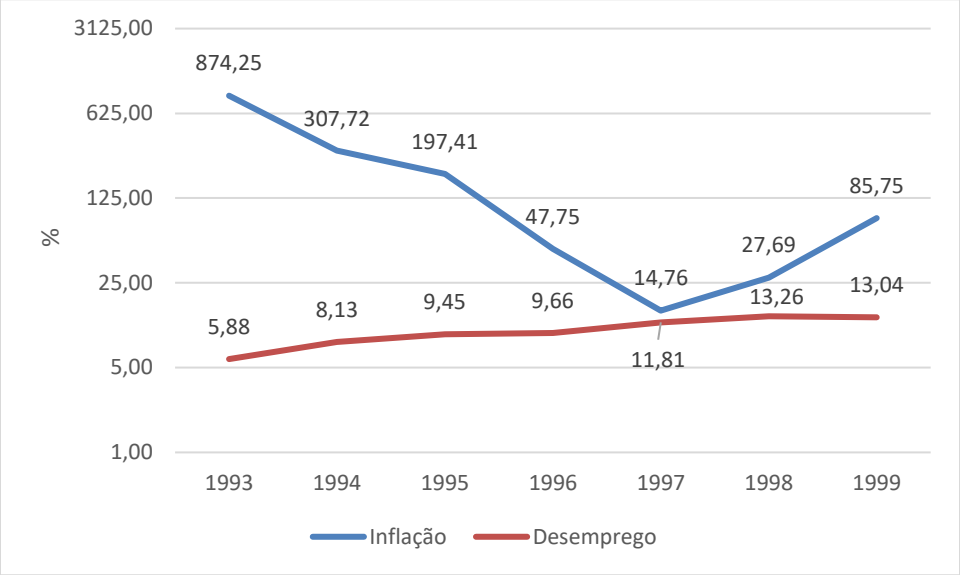
Gráfico 2 – Crescimento anual do PIB da Rússia, entre 1991 e 1999 (em %)

Fonte: World Bank (2020).

Conforme mostra o Gráfico 2, a Rússia registrou decréscimos significativos e ininterruptos do PIB ao longo de seis anos, com uma depressão econômica que chegou à marca de cerca de -15% em 1992. Após uma leve recuperação em 1997, a crise financeira de 1998 levou a economia russa a registrar novamente um decréscimo, de 5,3%. O relevante crescimento da economia em 1999 já demonstra a reação rápida após a crise, alavancada pela elevação dos preços do petróleo no mercado internacional, ainda que com inflação e nível de desemprego altos como será visto adiante.

A seguir o Gráfico 3 expõe a elevação dos preços na Rússia e a taxa de desemprego, com dados entre 1993 e 1999.

Gráfico 3 – Inflação e Nível de Desemprego na Rússia entre 1993 e 1999 (em %)



Fonte: World Bank (2020).

O Gráfico 3 mostra como a década de 90 foi um período de alta inflação na Rússia. Os dados, que começam na série histórica do Banco Mundial em 1993, iniciam com uma inflação anual de 874%, o que indica uma variação média mensal de quase 73% nos preços dos produtos russos naquele ano. Apesar de a trajetória ser de queda acentuada da inflação ao longo dos anos - a exceção dos anos de 1998 e 1999 em que são registradas novas acelerações devido à crise – a elevação anual de preços permaneceu alta, com fortes reflexos principalmente nas classes sociais mais baixas, as quais são mais impactadas pela elevação dos preços, dada a perda no poder de compra dos salários. Em relação ao nível de desemprego, o Gráfico 3 mostra que a Rússia apresentou uma alta sustentada, atingindo o patamar mais alto em 1998, com cerca de 13% de desempregados, dentre o total da força de trabalho do país.

As complicações derivadas da crise financeira sobre uma economia já abalada, resultaram novamente em uma crise política. Com um governo já desgastado, Yeltsin procurou a nomeação de um novo primeiro-ministro, o que ocasionou algumas trocas no cargo até a nomeação de Putin em 1999, então diretor do Serviço de Segurança Federal da Federação Russa (da sigla em russo, FSB), órgão que acumulou a maior parte das funções da extinta KGB, o serviço de inteligência soviético (SEGRILLO, 2012).

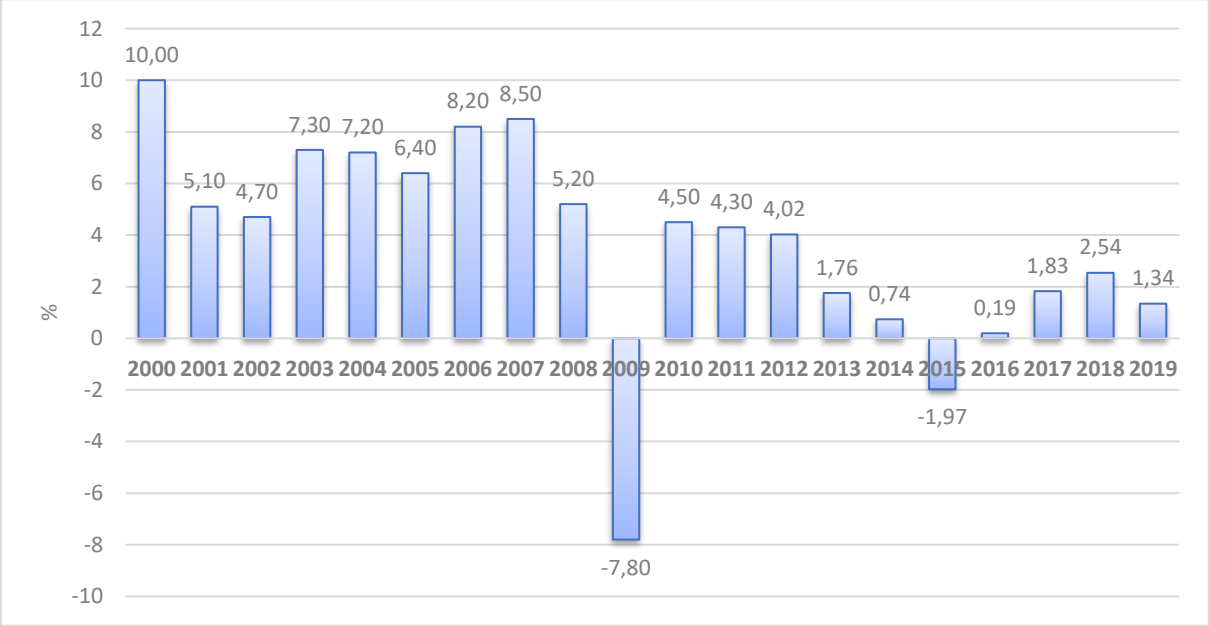
3.1.2 Período Putin/Medvedev (2000-Atual)

Alçado à primeiro-ministro, Putin logo viraria presidente da Rússia, quando no final do ano de 1999 Yeltsin anuncia a sua renúncia, algo que surpreendeu o país. No cargo de presidente interinamente, Putin concorre na eleição presidencial de 2000, quando então é eleito definitivamente para presidência do país.

O governo de Putin nos anos 2000 foi marcado por uma melhora significativa do ambiente econômico, impulsionado pelo período conhecido como *boom* das commodities, em que a forte elevação dos preços do petróleo e outros hidrocarbonetos no mercado internacional sustentou e permitiu o crescimento da economia de países que possuíam esses produtos em suas pautas de exportação, o que é o caso da Rússia (SEGRILLO, 2012).

A seguir são expostos os dados dos indicadores macroeconômicos do país durante os governos de Putin. O Gráfico 4 apresenta os dados do desempenho do PIB russo desde 2000.

Gráfico 4 – Crescimento anual do PIB da Rússia, entre 2000 e 2019 (em %)



Fonte: World Bank (2020).

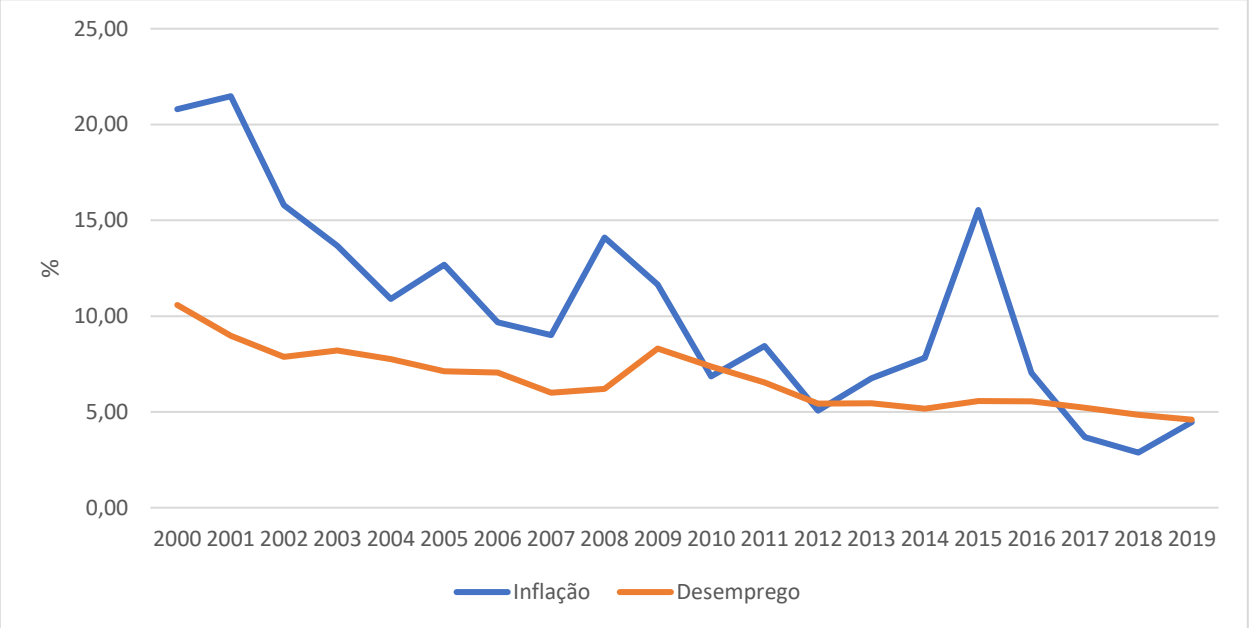
O Gráfico 4 mostra uma perspectiva essencialmente diferente da economia russa ao longo dos últimos dezenove anos, especialmente durante a primeira década do século. No período

conhecido como *boom* das *commodities* o país teve um crescimento elevado, somente sendo interrompido pela forte recessão de 2009, causada pela crise financeira mundial. Nos anos posteriores houve novamente o crescimento da economia, contudo percebe-se uma desaceleração do crescimento do PIB, como consequência da diminuição da cotação dos hidrocarbonetos internacionalmente, mostrando a intensa dependência que a economia russa possui dos preços internacionais das *commodities*, especialmente do petróleo e do gás.

No ano de 2015 foi registrada uma nova recessão da economia russa, resultado direto das sanções internacionais aplicadas sobre o país devido à anexação da Crimeia, então território ucraniano. Nos últimos anos a economia do país vem se recuperando, ainda que lentamente.

Abaixo o Gráfico 5 exibe os dados sobre as taxas de inflação e desemprego na Rússia entre 2000 e 2019.

Gráfico 5 – Inflação e Nível de Desemprego na Rússia entre 2000 e 2019 (em %)



Fonte: World Bank (2020).

No que tange ao índice de inflação anual, o Gráfico 5 mostra uma trajetória de controle dos níveis de preço, com duas interrupções que aparecem como picos no gráfico, registrados nos períodos de crise, em 2008 e 2015. Entretanto, mesmo os níveis mais altos de inflação registrados

nesse período mostram que a realidade dos níveis de preços na Rússia do século XXI em nada refletem o comportamento da inflação nos anos 90.

Assim como os outros indicadores econômicos analisados, a taxa de desemprego anual mostrada no Gráfico 5 corrobora na afirmação de que a economia do país se mostrou mais estável durante os governos de Putin.

A questão dos oligarcas que comandavam as principais indústrias russas e, portanto, tinham forte capacidade de interferência na economia e nas decisões políticas do país, foi também solucionada por Putin. Com a prisão de alguns dos maiores oligarcas condenados por crimes de corrupção e lavagem de dinheiro e a retomada do controle das indústrias pelo Estado, Putin foi visto pela opinião pública como um governante que seria capaz de estabilizar a Rússia (MIELNICZUK; PICCOLLI, 2015).

Com o crescimento do PIB e os sinais positivos vindos dos indicadores de emprego e da inflação, importantes fatores econômicos que promovem o apoio popular, Putin pôde focar em outros aspectos da política interna do país, tendo em vista que questões de segurança e de identidade nacional surgiram (MIELNICZUK; PICCOLLI, 2015).

A questão separatista na república da Chechênia voltou a ser foco de preocupações de Moscou ainda em 1999, com a ocorrência de ataques terroristas que se seguiram nos anos posteriores em vários lugares do território russo. O governo russo decidiu novamente invadir a região para neutralizar os grupos denominados como terroristas islâmicos por Moscou, reiniciando um conflito que tinha sido cessado anos antes. Contudo, dessa vez a forças russas conseguiram estabelecer um controle maior sobre a região, o que contribuiu para a popularidade de Putin na Rússia. Por outro lado, no plano externo, as ações foram muito contestadas dados os supostos crimes de guerra cometidos pelas forças armadas russas (SEGRILLO, 2012; SAKWA, 2008).

Ciente de que a questão identitária no país poderia voltar a ser foco de problemas internos, Putin promoveu uma reforma administrativa na configuração federativa da Rússia, retornando a um esquema de governo que provia maior poder decisório a Moscou, como forma de impedir dissidências, ainda que concessões fossem feitas como maneira de se manter a estabilidade do relacionamento entre o governo central e os entes da federação. A questão identitária na Rússia é um aspecto sensível para a unidade nacional, tendo em vista a pluralidade de povos que formam o país, bem como pelas diferentes denominações religiosas representadas (MIELNICZUK; PICCOLLI, 2015).

A principal resposta de Putin à essas questões foi um aumento do autoritarismo de seu governo, com o recrudescimento da narrativa da segurança nacional, que possuía respaldo pela ameaça representada pelos movimentos radicais da Chechênia, permitindo o acúmulo de poderes pelo Executivo russo para possibilitar a luta contra o terrorismo (SEGRILLO, 2012).

Com a regulação dos meios de imprensa e mídia de massa (muitos deles inclusive administrados direta ou indiretamente pelo governo), restringindo o alcance das críticas ao Kremlin, mudanças nas regras eleitorais, a repressão aos opositores políticos, além de um discurso nacionalista e de defesa dos valores tradicionais russo-ortodoxos, o governo Putin vem alcançando relativa estabilidade interna, permitindo a adoção de uma política externa mais ativa, como será mostrado a seguir (SEGRILLO, 2012; SAKWA, 2008).

Em 2008 assumiu a presidência da Rússia Dmitry Medvedev, tendo Putin sido indicado para o cargo de primeiro-ministro do país. Embora alguns analistas internacionais considerem que o mandato de Medvedev só tenha existido dada a limitação constitucional de dois mandatos consecutivos exercidos por Putin, deve ser considerado também que, por outros, Medvedev foi visto como alguém que poderia trazer um tom mais liberal e democrático para a Rússia (MAKARYCHEV, 201-?).

De acordo com Makarychev (201-?), as principais direções anunciadas por Medvedev giravam em torno de políticas de modernização e inovação do país, no combate a corrupção e na independência do sistema judiciário, ainda que muitas dessas promessas tenham sido vagas e não concretizadas de fato. Outras circunstâncias que marcaram o governo de Medvedev foram a crise financeira de 2009 que atingiu seriamente a economia russa e a guerra contra a Geórgia ainda no primeiro ano de seu mandato. No geral, apesar do tom mais liberal da figura de Medevdev, o seu mandato foi marcado mais por um período de continuidade do governo Putin do que por mudanças significativas na condução da política doméstica (MAKARYCHEV, 201-?).

No retorno em 2012 como presidente, o tom de Putin pode ser apresentado pelos pontos contidos em um documento apresentado em sua campanha, chamado de Manifesto do Milênio. Nele, Putin afirmou que identificou os problemas da sociedade e que pretendia resolvê-los por meio da implementação de quatro elementos fundamentais:

> 1) patriotismo integrativo, não se referindo apenas a um sentimento de nacionalismo, mas sim englobando convicções de orgulho da diversidade russa, de sua história e de sua posição no mundo; 2) gosudarstvennost (estadismo), a nação deveria ser sustentada a partir de uma autoridade política forte, capaz de manter a integridade, a ordem interna e afirmar os interesses externos do país; 3) patriotismo pragmático, a nação deve ser supra étnica, constitucionalmente homogênea e sem espaços para segmentações regionalistas;

> 4) solidariedade social, uma nação socialmente justa, prezando pelo bem-estar da população (SAKWA, 2008 apud MIELNICZUK; PICCOLLI, 2015, p. 52).

Fica claro, portanto, o teor nacionalista e unitário apregoado por Putin, além da centralização de poderes pelo Executivo, elementos que, aliado ao ótimo desempenho econômico da primeira década do século XXI, vem dando sustentação e estabilidade à política interna da Rússia. Nesse sentido, uma abordagem mais assertiva pode ser perseguida no âmbito externo, conforme será mostrado a seguir.

3.2 POLÍTICA EXTERNA

Durante a década de 90, no governo Yeltsin, a política externa russa refletia a instabilidade e as incertezas em que o país se encontrava. Nesse período três correntes teóricas competiam para determinar os rumos da política externa do país. O primeiro grupo, os *westernistas*, basicamente defendiam que a Rússia era uma nação ocidental e consideravam o Ocidente como o modelo civilizacional que mais havia progredido e, portanto, a política externa russa deveria estar alinhada com as potências ocidentais. O segundo grupo, os estatistas, enxergavam que o Estado russo tinha um papel fundamental na manutenção da ordem social e política nacionais e que a Rússia possui seu próprio modelo civilizacional de desenvolvimento. O terceiro grupo, os civilizacionistas, julgavam que a Rússia era uma civilização eurasiana, cujo modelo era superior e oposto ao ocidental, pela sua cultura e valores tradicionais (SVARIN, 2016).

Contudo, com a chegada de Putin ao poder e o período de estabilização da política interna, uma nova concepção de política externa ascendeu, com o principal objetivo de recolocar o país em uma posição de relevância no sistema internacional. A narrativa principal é de que a Rússia é uma nação de cultura, valores e tradições singulares, que sempre desempenhou papéis importantes nas relações internacionais e, logo, a sua posição como potência internacional é nada mais do que um aspecto natural, um direito originário (SVARIN, 2016).

Nesse sentido, o *status* de potência internacional percebido internamente – especialmente pelas elites dirigentes do país – deriva de uma percepção histórica baseada na Rússia Imperial e como principal integrante da URSS. Portanto, é notável que o *status* de potência, antes de necessariamente ser uma questão factual, deriva particularmente de uma construção social da elite

dirigente do país, o que se traduz na formação da política externa da Rússia, a qual é altamente centralizada nos mais altos escalões do Estado (MANKOFF, 2009).

Com essa perspectiva, esse item busca apresentar a analisar as principais nuances da política externa russa durante os governos Putin, mencionando também concepções vigentes durante a presidência de Medvedev (2008-2012), de modo a auxiliar na compreensão da arquitetura da política estratégica da Rússia no século XXI. Inicialmente é discutido brevemente sobre fundamentos gerais geopolíticos e normativos da política externa russa e, em seguida, como a deterioração das relações com o Ocidente inserem os EUA e a OTAN como ameaças à segurança nacional russa.

3.2.1 Fundamentos conceituais

Do ponto de vista geopolítico, a Rússia focaliza a sua atuação externa em três espaços geográficos: a Eurásia, o Euro-Atlântico e a Ásia-Pacífico (SVARIN, 2016).

A Eurásia, como conceito geopolítico, é extremamente importante para a construção da identidade e dos interesses nacionais da Rússia, uma vez que ela é considerada pelo país como a sua zona tradicional de influência. O espaço é constituído basicamente pela própria Rússia e pelos países da Comunidade dos Estados Independentes (CEI), uma organização internacional formada pela maior parte das ex-repúblicas soviéticas e cujas decisões políticas possuem forte influência de Moscou, funcionando como um mecanismo político para a projeção de poder da Rússia na sua vizinhança. A existência da Eurásia como um espaço geopolítico formal ainda é teorizada, tendo em vista que a Rússia ainda não foi capaz de consolidar quais são características diferenciais que a região apresenta, sendo esse inclusive um dos objetivos da política externa do país (SVARIN, 2016).

O espaço Euro-Atlântico, por sua vez, é a região que congrega os países da Europa ocidental, os EUA e o Canadá e pode ser representada por duas organizações: a União Europeia e a OTAN. Atualmente, a Rússia se sente excluída do concerto de países europeus e, ao mesmo tempo, pressionada para fora da ordem mundial multipolar, devido, segundo a Rússia, ao comportamento hostil dos EUA e da OTAN - com a conivência da UE (SVARIN, 2016; STONE, 2017).

O espaço da Ásia-Pacífico, por fim, concentra os países do leste e sudeste asiático, região que registrou o maior crescimento econômico do planeta nas últimas duas décadas, especialmente devido aos Tigres Asiáticos e a China, a qual se tornou a segunda maior potência econômica mundial. O interesse russo decorre principalmente da oportunidade de mercado advinda do crescimento acelerado desses países, dada a relevância da Rússia como exportadora de *commodities* energéticas. Ademais, a formação de alianças com esses países pode servir como contraponto à influência dos países ocidentais, fortalecendo a posição da Rússia no cenário internacional (SVARIN, 2016).

Da ótica do direito internacional, a Rússia é uma forte defensora do princípio da soberania, rechaçando quaisquer tentativas de flexibilização desse conceito, uma das principais bases do atual sistema de Estados nacionais. Além disso, defende os mecanismos da Organização das Nações Unidas (ONU), principalmente a autoridade do Conselho de Segurança (CS), no qual ela é membro permanente, o que lhe confere poder de veto nas questões de segurança internacional. Entretanto, os posicionamentos da Rússia decorrem fortemente de uma posição defensiva e de manutenção de seu *status* político de potência internacional (DE HAAS, 2010).

As tentativas de reformas do princípio da soberania são constantemente vistas pela Rússia como atentatórias ao regime político e social do país, portanto entendidas como uma questão de segurança nacional. A defesa da autoridade do CS, por outro lado, serve como contraponto às ações unilaterais dos EUA no plano internacional e buscam reforçar a relevância da Rússia para os assuntos de manutenção da paz e segurança internacionais (DE HAAS, 2010).

No que tange aos nortes gerais da política externa, o Conceito de Política Externa (CPE) da Federação Russa de 2016 traz os seguintes objetivos:

> a) Garantir a segurança nacional, a soberania e a integridade territorial e fortalecer o Estado de Direito e as instituições democráticas;
> b) Criar um ambiente externo favorável que permitiria à economia da Rússia crescer de forma constante e se tornar mais competitiva e promover a modernização tecnológica, bem como padrões de vida e qualidade de vida mais elevados para sua população;
> c) Consolidar a posição da Federação Russa como centro de influência no mundo de hoje;
> d) Fortalecer a posição da Rússia nas relações econômicas globais e prevenir qualquer discriminação contra bens, serviços e investimentos utilizando as opções oferecidas por organizações econômicas e financeiras internacionais e regionais;
> e) Promover ainda mais os esforços para fortalecer a paz internacional e garantir a segurança e estabilidade globais com vistas a estabelecer um sistema internacional justo e democrático que trate as questões internacionais com base na tomada de decisão coletiva, o Estado de Direito Internacional, principalmente

> as disposições do Carta das Nações Unidas (Carta das Nações Unidas), bem como relações igualitárias de parceria entre os Estados, tendo o papel central e coordenador da Organização das Nações Unidas (ONU) como órgão-chave encarregado de regular as relações internacionais;
> f) Buscar relações de vizinhança com Estados adjacentes, auxiliá-los na eliminação das existentes e prevenir o surgimento de novos focos de tensão e conflitos em seu território; g) promover, em estruturas bilaterais e multilaterais, parcerias mutuamente benéficas e iguais com países estrangeiros, associações interestaduais, organizações internacionais e dentro de fóruns, guiadas pelos princípios de independência e soberania, pragmatismo, transparência, previsibilidade, uma abordagem multidirecional e o compromisso de perseguir prioridades nacionais em uma base não confrontacional; expandir a cooperação internacional em uma base não discriminatória; facilitar o surgimento de alianças de rede e a participação pró-ativa da Rússia nelas;
> g) Assegurar a proteção abrangente e efetiva dos direitos e interesses legítimos dos cidadãos russos e compatriotas residentes no exterior, inclusive no âmbito de várias estruturas internacionais;
> h) Fortalecer o papel da Rússia na cultura internacional; promover e consolidar a posição do idioma russo no mundo; levantar a consciência global das realizações culturais da Rússia e legado histórico nacional, identidade cultural dos povos da Rússia e educação e pesquisa russas; consolidar a diáspora de língua russa;
> i) Para reforçar a posição da mídia de massa russa e ferramentas de comunicação no espaço de informação global e transmitir a perspectiva russa do processo internacional para uma comunidade internacional mais ampla;
> j) Facilitar o desenvolvimento de um diálogo construtivo e de parceria com vistas a promover a harmonia e o enriquecimento mútuo entre várias culturas e civilizações (RUSSIA, 2016, s/p, tradução própria).

Portanto, nota-se que a Rússia deseja se envolver de forma ampla em diversas agendas internacionais, buscando uma participação ativa e deliberante. Ao mesmo tempo, reforça instituições como a soberania e a legitimidade e força normativa do direito internacional e o direito de defesa do povo russo fora das fronteiras nacionais. Por fim, traz ainda a necessidade de fortalecer o papel da mídia russa fora do país, em um claro contraponto a influência da informação pelas mídias ocidentais dentro e fora da Rússia.

3.2.2 Relações com outros atores: EUA e OTAN

Nos primeiros anos do governo de Putin a Rússia manteve uma relação relativamente amistosa com as potências ocidentais, em muito alicerçada em um elemento comum aos EUA e à Rússia no período: o combate ao terrorismo islâmico ou a ‘Guerra ao Terror’. Os atentados terroristas de 11 de setembro nos EUA - em um momento em que a Rússia já vivia problemas com o terrorismo em seu próprio país - fez com que o país se posicionasse de forma favorável a uma

reação estadunidense contra a Al Qaeda no Afeganistão, inclusive oferecendo apoio logístico (MANKOFF, 2009; STONE, 2017).

No entanto, a boa relação com os EUA não durou muito. Ações tomadas por ambos os lados criaram um clima de desconfiança e animosidade, pautada em uma visão, pelo Ocidente, de uma Rússia imperialista, com fortes tendências de expansão territorial sobre o leste europeu. E por outro lado, de uma visão russa de que o Ocidente, em especial os EUA, trabalham constantemente para impedir a Rússia de se consolidar como um Estado influente no sistema internacional, preferindo tratá-la como um país periférico (MANKOFF, 2009).

De acordo com Mankoff (2009), apesar de o comportamento da política externa russa ao final dos anos 90 já indicar um desencontro entre o Ocidente e a Rússia em termos de agenda de segurança (como foi o caso da Guerra do Kosovo), alguns acontecimentos ao longo dos anos 2000 resultaram em um novo clima de suspeição entre EUA/OTAN e Rússia, conforme mostra o Quadro 3.

Quadro 3 – Ações que contribuíram para o afastamento da Rússia em relação ao Ocidente

Ações dos EUA/OTAN	Ações da Rússia
Apoio às Revoluções Coloridas e críticas em relação as ações russas na Chechênia.	Interrupção do fornecimento de gás para a Ucrânia (2006) e o comportamento hostil em relação aos países bálticos.
Alargamento da OTAN em direção ao leste europeu, particularmente para países que estão no entorno estratégico da Rússia.	Acusações de assassinatos de críticos do Kremlin (2006) e supressão da oposição política russa em geral.[10]
Projetos para a instalação do escudo antimíssil na Europa.	Nacionalização de companhias de gás e petróleo ocidentais.

Fonte: Elaborado pelo autor com base em Mankoff (2009).

Desacreditada com as intenções estadunidenses, a Rússia passa a apresentar uma política externa mais assertiva, o que se traduziu em mudanças importantes na versão de 2008 do Conceito de Política Externa da Federação Russa, como a priorização das relações russas com a Europa e a leitura dos EUA como um Estado desestabilizador do sistema internacional, cujas ações produzem ameaças à segurança russa (RUSSIA, 2008). A guinada na política externa russa se reflete inclusive

[10] Assassinato a tiros da jornalista Anna Politkovskaya (2006) e do político Boris Nemtsov (2015) e o envenenamento do ex-agente da KGB Aleksandr Litvinenko (MANKOFF, 2009; BBC, 2015).

em termos da segurança energética, com os gasodutos que fornecem o gás russo a Europa e suas indústrias possuindo um papel estratégico de relevância para a manutenção da influência da Rússia sobre os países de trânsito no leste europeu e, também, como recurso-chave nas negociações com a Europa (PICCOLLI, 2012).

Na gestão de Medvedev, foi procurada uma reaproximação com a UE, inclusive com a proposta de um acordo que beneficiaria o desenvolvimento e a modernização da Rússia. A própria figura de um governante mais liberal percebida pelo Ocidente no início de seu mandato auxiliou com que houvesse algumas manobras de realinhamento. No entanto, as relações entre a Rússia e o Ocidente viriam novamente a serem estremecidas com a Guerra Russo-Georgiana ainda em 2008 e a continuidade do projeto de instalação do escudo antimísseis pelos EUA e a OTAN (MOSHES, 2012).

A Rússia permaneceu irredutível em sua postura de reafirmar os seus interesses nacionais, notadamente relacionados com a restauração e manutenção da influência russa em seu entorno estratégico, constituído essencialmente pela CEI. Além disso, a insistência europeia em implementar uma rede de defesa antimísseis com parte do *hardware* militar instalado no leste europeu, foi entendido como uma ameaça ao equilíbrio de poder na região e à dissuasão estratégica, uma vez que a Rússia estaria impossibilitada de responder simetricamente à um possível ataque por parte da OTAN (MOSHES, 2012; STONE, 2017).

Em sua versão de 2016, o primeiro CPE após o retorno de Putin a presidência da Rússia mostra que o país observa o retorno da militarização e uma maior instabilidade nas relações entre os Estados, ainda que mencione a função do desenvolvimento de capacidades de *soft power* para atingir os seus objetivos de política externa. Tal indicação demonstra que a Rússia permanece empenhada em reforçar o seu aparato militar, mas também explica os recentes posicionamentos do país em matéria diplomática, econômica, científica, ambiental e humanitária, por exemplo (RUSSIA, 2016b).

Segundo Bogdanova (2016), a abordagem de *soft power* da Rússia difere em essência do entendimento cunhado por Nye. Para a autora, a Rússia se utiliza de recursos de *soft power* com fundamento nos seus interesses geopolíticos e de modo reativo às ações do Ocidente, sendo este um importante fator para explicar o comportamento do país em relação ao mundo. Outro aspecto que Bogdanova (2016) destaca é o caráter instrumental do *soft power* como suporte para o *hard*

power na concepção russa, o que demonstra que a política externa do país emprega essas duas dimensões de poder de forma articulada.

Enquanto a Rússia persegue uma agenda internacional ampla, o relacionamento do país com as potências ocidentais vem se deteriorando ainda mais ao longo da última década. Utilizando-se de uma retórica defensiva, baseada em atitudes reativas ao que Putin trata como atos desestabilizadores e atentatórios à segurança nacional russa (STONE, 2017).

Portanto, e conforme assinala Giles (2016a), a Rússia vem empreendendo ações que buscam minar a capacidade do Ocidente, especialmente dos EUA e da OTAN em constranger a consolidação da Rússia como uma potência internacional. É notável que a postura defensiva adotada pelo país se reflete em atividades que projetam o poder da Rússia para regiões para além do seu entorno estratégico.

Nesse sentido, conforme mostram Connel e Vogler (2017), como será melhor trabalhado no Capítulo 4, uma série de campanhas externas foram postas em prática, as quais vão de encontro a agenda de segurança dos EUA e da Europa, como são exemplos os ataques cibernéticos contra a Estônia (2007), a guerra contra a Georgia (2008), a anexação da Crimeia e os conflitos na Ucrânia (2014-atual) e as reiteradas acusações sobre ingerências em processos políticos internos na Europa, mas especialmente nas eleições estadunidenses de 2016.

Ao se considerar todas as questões apresentadas sobre a política externa da Rússia nos governos Putin, é possível analisar que a estratégia de inserção internacional russa se baseia nas duas vertentes teóricas de relações internacionais, isto é, o realismo e o construtivismo. No que concerne ao posicionamento do país, é notável que a Rússia se entende inserida em um sistema de Estados anárquico, em que as relações de poder imperam e a estratégia de inserção deve buscar o aumento do poder relativo do país. Por outro lado, a narrativa que sustenta essa estratégia tem origem na construção social do *status* de potência, uma consequência da concepção do que as elites do país representadas por Putin refletem sobre a participação da Rússia nos assuntos internacionais. Desse modo, o aparente desapreço do Ocidente pela figura da Rússia como grande potência motiva o país a buscar a sua consolidação internacional por meio de uma retórica defensiva, embasada no resguardo do seu *status* que estaria ameaçado pelas investidas ocidentais, particularmente dos EUA e da OTAN.

3.3 POLÍTICA DE SEGURANÇA NACIONAL E DEFESA

Com base no que foi apresentado no item anterior, este subcapítulo versará sobre a política de segurança nacional e defesa da Rússia, com ênfase para o período pós-2010, tendo como fundamento a Doutrina Militar (DM), a Estratégia de Segurança Nacional (ESN) e a Doutrina de Segurança da Informação (DSI), promulgadas respectivamente em 2014 e 2015 e 2016.

Inicialmente será analisado o contexto de percepção de ameaça segundo a Rússia, onde é novamente destacada a relação com os EUA e a OTAN e a visão destes atores como desestabilizadores do sistema internacional. Em seguida, é tratado como o ciberespaço é entendido pela Rússia no âmbito de sua política de segurança e defesa, no qual a informação é considerada o elemento primordial para a compreensão da temática. Por fim, é colocada em perspectiva a nova doutrina militar-estratégica da Rússia, em que são discutidos os princípios estratégicos norteadores que embasam o seu conceito operacional de guerra, apresentado e discutido no item 3.4.

3.3.1 Percepção de ameaça

Conforme mencionado anteriormente, a Rússia percebe o cenário internacional e se coloca nele de forma caracteristicamente realista, como um ator internacional que procura a sua preservação e de seus interesses em mundo marcado pelo aumento da instabilidade regional e global. Para a Rússia, a conjuntura atual do sistema internacional é a de um período de transição de uma ordem mundial unipolar para uma ordem multipolar, processo esse que está tornando mais visíveis as contradições existentes no sistema em relação ao desenvolvimento mundial com o aprofundamento das desigualdades socioeconômicas entre os países, além das disputas por recursos, mercados e do controle sobre as principais rotas do comércio internacional. Segundo o país, a evidência dessas contradições está acirrando a competição entre as nações por modelos e estratégias de desenvolvimento, através do aproveitamento das capacidades dos recursos humanos, científicos e tecnológicos (RUSSIA, 2015).

Além disso, existe a percepção de um ambiente internacional em que o acirramento crescente entre os Estados pode levar a um novo Dilema de Segurança, uma vez que a Rússia enxerga uma nova tendência a militarização e utilização da força no sistema internacional, conforme consta na ESN de 2015:

> O papel da força como fator nas relações internacionais não está diminuindo. A aspiração de construir e modernizar armas ofensivas e desenvolver e implantar novos tipos está enfraquecendo o sistema de segurança global e também o sistema de tratados e acordos na esfera de controle de armas. Os princípios de segurança igual e indivisível não estão sendo observados nas regiões euro-atlântica, euro-asiática e Ásia-Pacífico. Os processos de militarização e corrida armamentista estão se desenvolvendo em regiões adjacentes à Rússia (RUSSIA, 2015, s/p, tradução própria).

Ao se referir ao escopo geopolítico Euro-Atlântico, a Rússia dirige críticas ao comportamento da OTAN, a qual estaria reiteradamente desrespeitando os dispositivos legais internacionais através de suas atividades militares, especialmente ao realizar o aprimoramento das capacidades militares dos seus países membros, em conjunto com uma estratégia de expansão do bloco e de seus recursos de força para localidades próximas às fronteiras russas. Portanto, conforme já mencionado, a política da OTAN é vista como uma ameaça para a segurança nacional russa (RUSSIA, 2015).

Entretanto, não é somente na figura da OTAN que as ações das potências ocidentais perturbam a Rússia e seus interesses nacionais. De acordo com a ESN (2015), o Ocidente continuadamente pratica ações que buscam minar os processos de integração regionais que o país arquiteta, além de criar núcleos de tensões em porções do globo. Ademais, a atuação do Ocidente procura posicionar a Rússia como um país inimigo, passando a imagem de um Estado hostil para as populações do leste europeu (RUSSIA, 2015).

O terrorismo também é citado como uma consequência das ingerências do Ocidente, tendo em vista que a desestabilização de governos nacionais, o auxílio à grupos armados e o engendramento de conflitos em alguns países para forçar a troca de regimes políticos está criando vácuos de poder que possibilitam o surgimento e fortalecimento de grupos terroristas. Ainda segundo o entendimento da Rússia, as instabilidades regionais geradas pelas interferências ocidentais já são sentidas por esses países, haja vista as ondas migratórias de refugiados que chegam ao litoral europeu, vindos de países da região do Maghreb[11] e do Oriente Próximo e Médio atingidos pela instabilidade da política doméstica e por conflitos armados internos (RUSSIA, 2015).

A questão nuclear é outro aspecto que representa riscos à segurança internacional e à segurança nacional russa, de acordo com a visão do país. Tal constatação se deve pela leitura de

[11] De acordo com a Enciclopédia Britannica, o Maghreb corresponde a "região do Norte da África que faz fronteira com o Mar Mediterrâneo" (BRITANNICA, c2021).

que atualmente existe o perigo potencial de novos atores internacionais deterem capacidades nucleares, além da proliferação de outros elementos capazes de desenvolverem armas de destruição em massa, como é o caso das armas químicas e biológicas (RUSSIA, 2015).

Finalmente, é caracterizado como uma ameaça para segurança nacional da Rússia a utilização dos elementos do espaço da informação – ou meio cibernético - como ferramentas para o alcance de objetivos geopolíticos por parte de alguns países. Conforme salientado na ESN da Rússia, as tecnologias da informação e comunicação estão sendo empregadas para fins políticos, "inclusive por meio da manipulação da consciência pública e da falsificação da história, está exercendo uma influência crescente sobre a natureza da situação internacional" (RUSSIA, 2015, s/p, tradução livre).

Diante dessa realidade entendida como repleta de incertezas e instabilidades, a Rússia busca a sua autopreservação e, para mitigar os riscos à segurança nacional, estaria, de acordo com o país:

> concentrando esforços no fortalecimento da unidade interna da sociedade russa, garantindo estabilidade social, acordo interétnico e tolerância religiosa, eliminando desequilíbrios estruturais e modernizando a economia e melhorando a capacidade de defesa do país (RUSSIA, 2015, s/p, tradução própria).

Além disso, o fortalecimento de alianças com outros países como forma de contraponto à OTAN faz parte dos projetos de segurança da Rússia, conforme reforça a DM da Federação Russa (2014). Nesse sentido o documento menciona a Organização do Tratado de Segurança Coletiva (OTSC) - uma aliança militar que congrega além da própria Rússia alguns outros países do seu entorno estratégico - e a Organização para Cooperação de Xangai (OCX), em que também está presente a República Popular da China. As duas entidades formam um importante cordão de segurança coletiva que abrange a região euroasiática (RUSSIA, 2014).

3.3.2 Espaço da informação: ameaças e oportunidades

Inicialmente, é importante esclarecer que os termos "ciberespaço" ou "espaço cibernético" são esparsamente utilizados pelos teóricos-estrategistas russos, pela academia ou pelos documentos oficiais para se referir ao domínio cibernético, a exceção das citações russas à bibliografia ocidental sobre a matéria. No lugar da referência ao espaço cibernético, a bibliografia russa utiliza o termo "espaço da informação" ou "esfera da informação" (CONNELL; VOGLER, 2017; GILES, 2016a). A diferença de tratamento se deve, especialmente, à importância que a Rússia dá aos aspectos informacionais, tidos como elementos essenciais para a manutenção das instituições do Estado

russo, da sociedade civil e da segurança nacional, bem como, são ativos de importância para os interesses nacionais do país, o que pode ser constatado por meio das recentes doutrinas nacionais publicadas nas áreas de segurança e defesa.

Nessa perspectiva, a esfera da informação, na concepção da DSI de 2016, é definida:

> como uma combinação de informações, objetos de informatização, sistemas de informação e *sites* na rede de informações e telecomunicações da Internet (doravante denominada "Internet"), redes de comunicações, tecnologias da informação, entidades envolvidas na geração e processamento de informações, desenvolvimento e uso as tecnologias acima e, em garantir a segurança da informação, bem como um conjunto de mecanismos que regulam as relações públicas na esfera (RUSSIA, 2016a, s/p, tradução própria).

Na concepção russa, a utilização do termo "espaço da informação" visa abranger e compreender tanto os fatores técnico-computacionais - que tornam possível a operacionalização do meio virtual - quanto os fatores informacionais-psicológicos – que se referem à criação, transmissão e a assimilação das informações no meio cibernético, bem como, dos efeitos de consciência sobre o público que podem ser gerados a partir disso. Tal fato demonstra que a Rússia possui uma visão mais abrangente do domínio, quando comparado com as concepções ocidentais de ciberespaço (GILES, 2016a; CLAESSEN, 2020).

A análise que se extrai dessa interpretação permite apontar que o país possui uma compreensão dual sobre a instrumentalização do ciberespaço no que concerne às políticas estratégicas nacionais. Sob um prisma, tem-se a função da informação como uma arma capaz de influenciar grupos e indivíduos e a internet como um ambiente de difusão e irradiação de informação sem fronteiras. De outra forma, a exploração do aspecto técnico-computacional, constituído essencialmente pelos *softwares*, principalmente os ligados aos sistemas ou infraestruturas críticos, também se traduz em capacidade de geração de efeitos adversos sobre a vida nacional. De todo o modo, percebe-se que a Rússia detém especial atenção para o controle sobre a informação como um ativo estratégico para o país.

Gerasimov (2013), Chefe do Estado Maior das Forças Armadas da Federação Russa, ao tratar sobre os aspectos atuais dos conflitos e da guerra moderna, afirma que os métodos conflitivos passaram a ser definidos por uma combinação de artifícios políticos, econômicos, informacionais, humanitários e outros não militares. O concerto desses instrumentos é acompanhado pela mobilização da população na forma de protestos, bem como, é:

> complementado por medidas militares secretas, incluindo a implementação da guerra de informação e as ações das forças de operações especiais. O uso aberto da força é muitas

> vezes disfarçado de manutenção da paz e solução de crises em certos momentos, principalmente para alcançar o sucesso final no conflito (GERASIMOV, 2013, s/p, tradução livre).

De acordo com Gerasimov (2013), as soluções de TIC não somente tornaram a comunicação em nível operacional entre as tropas e os comandos e órgãos de inteligência e controle mais rápidas e eficazes, diminuindo a capacidade do inimigo em tomar vantagem de possíveis vácuos de informação em confrontos militares diretos, mas são também um importante ativo para o rol de ações assimétricas. Conforme disserta o general:

> O confronto de informações abre amplas oportunidades assimétricas para reduzir o potencial de combate do inimigo. No norte da África, testemunhamos a implementação de impactos tecnológicos no governo e nas pessoas por meio de redes de informação. É necessário melhorar as ações no espaço da informação, incluindo a proteção de suas próprias instalações (GERASIMOV, 2013, s/p, tradução livre).

Ao mencionar o norte da África, Gerasimov (2013) refere-se diretamente aos acontecimentos da Primavera Árabe, série de movimentos populares organizados a partir das mídias sociais que engendraram a derrubada de regimes autoritários na região e, igualmente, resultaram em guerras civis e outros conflitos armados internos em algumas situações. Nesse ponto, a questão supramencionada sobre a ingerência ocidental nos assuntos de política interna de outros Estados, especialmente por parte dos EUA, observada pela Rússia e que a preocupa, volta à tona.

O potencial dos meios informacionais para fins geopolíticos se tornou aparente na perspectiva da Rússia nesses acontecimentos, sendo percebida uma mudança na abordagem da política externa dos EUA, o qual passou a adotar novos métodos para patrocinar a troca de regimes a contento dos seus objetivos geopolíticos. Charles Bartles (2016) faz uma leitura do entendimento da Rússia sobre a mudança do *modus operandi* das ações de interferência estadunidense e sintetiza esse pensamento, como segue:

> Em vez de uma invasão militar aberta, os primeiros ares de um ataque dos EUA vêm da parcela de uma oposição política por meio de propaganda do estado (por exemplo, CNN, BBC), Internet e mídias sociais e organizações não-governamentais (ONGs). Após incutir com sucesso dissidência política, separatismo e / ou conflito social, o governo legítimo tem dificuldade crescente em manter a ordem. À medida que a situação de segurança se deteriora, os movimentos separatistas podem ser estimulados e fortalecidos, e operações especiais não declaradas, forças militares convencionais e privadas (empresas que prestam serviços militares) podem ser introduzidas para combater o governo e causar mais estragos. Uma vez que o governo legítimo é forçado a usar métodos cada vez mais agressivos para manter a ordem, os Estados Unidos ganham um pretexto para a imposição de sanções econômicas e políticas, e às vezes até sanções militares, como zonas de exclusão aérea, para prender as mãos dos governos sitiados. e promover mais dissidência (BARTLES, 2016, p. 32, tradução própria).

Nesse sentido, nota-se que a Rússia percebe a existência de substancial relação entre as ações de ingerência, desestabilização e troca de regimes – responsáveis, em parte, pela atual conjuntura de instabilidade do cenário internacional - desempenhadas pelo Ocidente e, em particular, pelos EUA, e o emprego de recursos cibernéticos. Cabe ressaltar que a Rússia identifica que os instrumentos de informação são continuadamente utilizados para atingir a população russa, em especial visando destruir os "valores morais e espirituais tradicionais russos" (RUSSIA, 2016a, não paginado, tradução própria).

A DSI de 2016, em seu artigo 12 (doze), tratando das provisões gerais do documento, apresenta um trecho que corrobora com a tese de Bartles sobre a compreensão russa em relação ao emprego dos recursos de poder cibernético para fins políticos:

> 11. Os serviços de inteligência de certos Estados estão usando cada vez mais informações e ferramentas psicológicas com o objetivo de desestabilizar a situação política e social interna em várias regiões do mundo, minando a soberania e violando a integridade territorial de outros Estados. Organizações religiosas, étnicas, de direitos humanos e outras organizações, bem como grupos separados de pessoas, estão envolvidas nessas atividades e as tecnologias da informação são amplamente utilizadas para esse fim. (RUSSIA, 2016a, s/p, tradução própria).

Os artigos 15 e 16 do mesmo documento trazem outras considerações no âmbito da defesa nacional, do Estado e da segurança social, discorrendo sobre a utilização dos recursos de poder cibernético para o alcance de objetivos militares e políticos por parte de alguns Estados, incluindo instrumentos de *hard power*, como pode ser notado:

> 15. A segurança da informação na esfera da defesa nacional é caracterizada pelo crescente uso por certos Estados e organizações de tecnologias da informação para fins militares e políticos, inclusive para ações inconsistentes com o direito internacional e procuram minar a soberania, a estabilidade política e social e a integridade territorial da Federação Russa e de seus aliados, e representam uma ameaça à paz internacional, à segurança global e regional.
> 16. A segurança da informação na esfera do Estado e da segurança social é caracterizada por um aumento contínuo na complexidade, escopo e coordenação de ataques de computador a objetos de infraestrutura de informações críticas, atividades aprimoradas de inteligência de Estados estrangeiros contra a Federação Russa, além de riscos crescentes de que as tecnologias da informação serão usadas para violar a soberania, a integridade territorial ou a estabilidade política e social da Federação Russa (RUSSIA, 2016, s/p, tradução própria).

Além dos esforços para a securitização do meio cibernético, devido às ameaças existentes, a Rússia também constata esse meio como um ambiente importante para ações ofensivas, no escopo de sua estratégia de defesa nacional. Tal entendimento deve-se, particularmente, pelas capacidades que podem ser desenvolvidas através do emprego dos recursos cibernéticos, principalmente em

termos de ações assimétricas (como forma de compensar a inferioridade das forças convencionais russas em relação aos contingentes dos EUA e OTAN) e atividades ofensivas dotadas de maior discrição, diminuindo a capacidade do inimigo em atribuir ao país a responsabilidade por ataques, o que reduz as chances de retaliações e escalonamento de conflitos (CONNEL; VOGLER, 2017).

Em síntese, a preocupação da Rússia com o domínio cibernético possui um caráter fortemente alicerçado na forma com que o país observa as ações dos países ocidentais, em especial dos EUA, na utilização dos recursos cibernéticos para obtenção de resultados que satisfaçam os objetivos de política externa, particularmente no enfraquecimento e desestabilização de governos adversários, representando também uma ameaça para a estabilidade e a segurança nacional russa. Portanto, a percepção da Rússia de que os recursos cibernéticos representam uma ameaça para a segurança nacional e para a sua posição no cenário internacional, quando dominados e utilizados por seus adversários geopolíticos, manifesta a postura do país em empregar esses instrumentos a partir de uma retórica defensiva (AYRES PINTO et al, 2020).

3.3.3 Nova doutrina militar-estratégica

Nesse sentido, a DM de 2014 introduz pela primeira vez nos tempos pós-soviéticos nos documentos militares oficiais do país o conceito de dissuasão não-nuclear, isto é, o emprego de métodos militares convencionais ou não militares, de forma estratégica, de modo a intimidar e desmotivar agressões por parte de inimigos (RUSSIA, 2014).

Durante a década de 90 e um período dos anos 2000 a dissuasão estratégica da Rússia permaneceu unicamente atrelada às suas capacidades nucleares, visto que as forças convencionais se encontravam debilitadas, com problemas de gestão graves e equipamentos ultrapassados, colocando a Rússia em posição de inferioridade militar em relação aos EUA e a OTAN. Dessa maneira, os estrategistas russos conceberam o modo clássico de dissuasão estratégica – o nuclear – como a principal instituição de defesa do país, dado o amplo arsenal nuclear herdado da URSS (VEN BRUSSGAARD, 2016).

Contudo, com a reestruturação e requalificação das forças convencionais (ainda em curso), em conjunto com a percepção no meio militar de que as guerras modernas são conduzidas com táticas que mesclam e integram o emprego de recursos militares e não-militares, a Rússia concebeu um novo conceito de dissuasão estratégica. O novo conceito de dissuasão estratégica não é

inteiramente defensivo, sendo válido o emprego ofensivo de instrumentos nucleares, não-nucleares e não-militares, tanto em tempos de paz quanto de guerra, com o objetivo de "conter, dissuadir e coagir" o inimigo para se sobressair no conflito (VEN BRUSSGAARD, 2016).

Nesse contexto, os recursos cibernéticos são elementos adicionais no conjunto de capacidades militares e não-militares russas para alcançar os seus objetivos geopolíticos – que inclui também a utilização da política/diplomacia, da pressão econômica e da ciência. O conceito de 'dissuasão estratégica', de acordo com os estrategistas-militares russos é operacionalizado por um processo que eles denominam de "*voina novogo tipa*" ('novo tipo de guerra'), trabalhado a seguir. (THORNTON; MIRON, 2019, p. 258-259).

3.4 ASPECTOS INSTITUCIONAIS E OPERACIONAIS DO EMPREGO DE RECURSOS CIBERNÉTICOS

Conforme o tratado no subcapítulo 3.3, a Rússia demonstra uma relevante preocupação com como o espaço da informação pode ser utilizado para fins políticos por outros países contra ela. No mesmo contexto, foi mostrado como a nova doutrina militar-estratégica russa passa a contemplar elementos não-cinéticos como parte de uma estratégia ofensiva para garantir a segurança nacional do país.

Desse modo, o presente subcapítulo se debruça sobre as capacidades e estratégias da Rússia para atuar no domínio cibernético. Para tanto, são elencados e analisados os principais organismos identificados pertencentes à estrutura oficial do Estado russo (além de outras instituições) que realizam operações no ciberespaço.

Ao final, o componente cibernético é inserido no arquétipo da Guerra Híbrida (GH), de modo a elucidar como os recursos cibernéticos russos são, de fato, implementados no contexto operacional dos conflitos por parte da Rússia.

3.4.1 Burocracia e institucionalidade das capacidades cibernéticas

A divisão de competências cibernéticas dentro da burocracia russa não é muito clara, visto que esse é um assunto tratado de forma altamente confidencial pelo país. No entanto, algumas observações realizadas por agências de inteligência ocidentais e por pesquisadores da área

identificam a participação de órgãos da estrutura do Estado russo na instrumentalização e aplicação de recursos cibernéticos contra alvos ocidentais (CONNEL; VOGLER, 2017; GILES, 2016b; MUELLER, 2019; USA, 2019).

Na estrutura organizacional de inteligência e segurança da Rússia existem atualmente quatro órgãos principais, todos criados com atribuições incorporadas da KGB soviética (com exceção do último, que já existia na estrutura do Estado soviético), são eles:

- O Serviço de Segurança Federal (da sigla em russo, FSB), oficialmente responsável pela segurança e operações de inteligência no âmbito interno;
- O Serviço de Inteligência Externa (da sigla em russo, SVR), oficialmente responsável pelas operações de inteligência fora das fronteiras nacionais;
- O Serviço de Proteção Federal (da sigla em russo FSO), oficialmente responsável pela segurança das autoridades do Estado (GALEOTTI, 2016);
- Diretório Central de Inteligência (da sigla em russo, GRU), oficialmente responsável pelas operações de inteligência militar.

Dentre esses quatro órgãos, o FSB e o GRU são os mais citados por estudos e relatórios técnicos e de inteligência como operadores das capacidades cibernéticas russas, desse modo, esse trabalho se atém a analisar somente esses dois organismos.

O FSB é o principal órgão de segurança da Rússia, tendo papel fundamental na elaboração das Doutrinas de Segurança da Informação do país e com participação destacada no Conselho de Segurança da Rússia, órgão responsável pelo aconselhamento do presidente para questões relativas à segurança nacional. Há igualmente o respaldo político dessa influência, dado que cadeiras de relevância no governo são ocupadas também por ex-funcionários do FSB, como é o caso de Putin (GALETOTTI, 2016).

Além disso, a incorporação em 2003, por meio de decreto presidencial, da Agência de Comunicações e Informações do Governo Federal (da sigla em russo, FAPSI) – o órgão de inteligência eletrônica da Rússia - pelo FSB acabou fortalecendo mais a posição do órgão e aumentando a sua capacidade técnica de atuação no meio cibernético. Um ano antes, em 2002, houve uma reestruturação do departamento de inteligência cibernética do FSB, ocorrendo uma troca de nome, passando a ser chamado de Centro de Segurança da Informação (SOLDATOV; BOROGAN, 2018; GALEOTTI, 2016).

Outrossim, a estratégia de emprego de recursos cibernéticos pela Rússia também envolve a terceirização de competências, principalmente por meio de relações com entes não institucionais, sob coordenação do FSB. A utilização de equipes de *hackers* e outros recursos não diretamente ligados às estruturas do Estado russo servem como forma de dificultar a atribuição dos ataques cibernéticos e de outras ingerências geradas a partir do ciberespaço (SOLDATOV; BOROGAN, 2018).

Contudo, conforme explicam Connel e Vogler (2017) e Giles (2016b) após a Guerra da Geórgia de 2008, a preocupação com a performance das forças armadas russas – dado os erros em nível tático e operacional durante a campanha na região – fez com que fossem realizados novos investimentos no desenvolvimento das forças militares russas. A reestruturação e modernização das forças armadas do país foi realizada em conjunto com a criação de divisões especializadas em guerra de informação.

Nesse sentido, o GRU, órgão de inteligência militar, que dentre outras funções, coordena a atuação das forças militares de elite da Rússia (Spetsnaz), passou a possuir unidades dedicadas às CyberOps e InfoOps. A incorporação de capacidades cibernéticas por parte do aparato militar russo, de forma mais substancial, permitiu que os recursos cibernéticos se tornassem parte integrante do esforço militar da Rússia, sendo aplicados em conjunto com meios militares convencionais, como foi o caso das operações militares na Ucrânia em 2014 (CONNEL; VOGLER, 2017).

A seguir, o Quadro 4 relaciona as unidades do GRU que estariam envolvidas com atividades cibernéticas, de acordo com Bowen (2020).

Quadro 4 – Unidades do GRU supostamente envolvidas com atividades cibernéticas

Unidade do GRU	Descrição das operações
Unidade 26165	A Unidade 26165 foi estabelecida como o 85º Centro Principal de Serviços Especiais durante a Guerra Fria, responsável pela criptografia da inteligência militar. Frequentemente chamada de APT 28[12] ou Fancy Bear, a Unidade 26165 é uma das duas unidades identificadas pelo

[12] APT é a abreviação para *Advanced Persistent Threat*. De acordo com a Kaspersky (2021, s/p, tradução própria) "um ataque persistente avançado (APT) usa técnicas de *hacking* contínuas, clandestinas e sofisticadas para obter acesso a um sistema e permanecer nele por um período de tempo prolongado, com consequências potencialmente destrutivas".

	governo dos EUA responsáveis por hackear o Congresso Democrata Comitê de Campanha (DCCC), Comitê Nacional Democrático (DNC) e a campanha presidencial de Hillary Clinton.
Unidade 74455	A unidade 74455 parece ser uma unidade mais recente criada para ajudar a apoiar e expandir as capacidades cibernéticas do GRU. A unidade 74455 também é conhecida como o centro principal para tecnologias especiais e é comumente referida pelos relatos da mídia como *Sandworm*. Esta unidade cibernética está ligada a algumas das operações cibernéticas mais descaradas da Rússia, como o ataque NotPetya de 2017 na Ucrânia.
Unidade 54777	Esta unidade, também conhecida como 72º Centro de Serviços Especiais, é supostamente responsável pelas operações psicológicas do GRU. Isso inclui operar em apoio a outras unidades cibernéticas da GRU e operar no nível tático conduzindo guerra eletrônica e operações psicológicas.

Fonte: Adaptado de Bowen (2020).

De acordo com Galeotti (2016), apesar de o FSB e o GRU responderem oficialmente ao responsável pela administração presidencial (no caso do primeiro) e ao secretário do Conselho de Segurança (no caso do segundo), ambos os órgãos respondem de forma não oficial diretamente ao presidente da Rússia, Vladimir Putin.

Fora das estruturas civis e militares oficiais do Estado, outra entidade russa também possui um aprimorado arcabouço de competências cibernéticas, a Agência de Pesquisas na Internet (API). A API é uma entidade privada que estaria ligada a diversas InfoOps no meio cibernético em diferentes países nos últimos anos. De acordo com investigações conduzidas por um comitê especial do Senado dos EUA, a API é financiada por Yevgeniy Prigozhin, um oligarca russo que teria ligações com o Kremlin (USA, 2019).

A API estaria relacionada especialmente à utilização de *trolls*[13] e *bots*[14], com o objetivo principal de propagar nas redes sociais percepções e narrativas pró-russas ou benéficas aos objetivos políticos do Kremlin, de modo a influenciar grupos sociais específicos[15]. Segundo um artigo de 2015 publicado no *The New York Times* referenciado pelo relatório de investigação do do Senado dos EUA:

> [...] a API tinha cerca de 400 funcionários que trabalhavam em turnos de 12 horas, divididos entre vários departamentos, ocupando quase 40 salas. Os trolls criariam conteúdo em quase todas as redes de mídia social, incluindo LiveJournal, VKontakte (uma plataforma de mídia social baseada na Rússia modelada após o Facebook), Facebook, Twitter e Instagram. Os gerentes responsáveis por supervisionar os trolls monitoravam o local de trabalho por CCTV e eram "obcecados por estatísticas", como visualizações de página, postagens, cliques e tráfego (USA, 2019, p. 25, tradução própria).

Não menos importante são as mídias de informação russas, as quais também teriam contribuído com o trabalho relativo às InfoOps no exterior. Destaca-se o RT - inicialmente chamada de *Russia Today* - como um veículo de mídia de informação influente na Rússia e que distribui conteúdo informacional digital em seis línguas atualmente para mais de cem países (RT, [202-?]). De acordo com Sidorenko (2016), o RT é controlado pelo Estado russo e serve como um mecanismo estratégico de *soft power* cuja atuação é "desde promover explicitamente a Rússia, e o regime de Putin especificamente, até desacreditar o Ocidente" (SIDORENKO, 2016, p. 9, tradução própria). Como mostra a autora, a atuação do RT vem sendo criticada por instituições ocidentais, por supostamente promover um mau jornalismo e praticar campanhas de desinformação (SIDORENKO, 2016).

Outro veículo de mídia relevante é o Sputnik International, uma agência de notícias que sucede a RIA Novosti e o serviço de rádio Voice of Russia. A agência foi criada pelo grupo de mídia estatal Rossiya Segodnya e possui editorais com notícias locais em trinta países, inclusive no Brasil (SPUTNIK, 2021).

---

[13] De acordo com Klepper (2020, s/p, tradução própria): "A palavra troll uma vez se referia às bestas da mitologia escandinava que se escondiam sob as pontes e atacavam os viajantes. Agora, também se refere a pessoas que fazem postagens *online* para provocar outras pessoas, às vezes para sua própria diversão e às vezes como parte de uma campanha coordenada."

[14] Ainda segundo Klepper (2020, s/p, tradução própria): "Os soldados de infantaria descartáveis neste conflito digital são *bots*. No contexto da mídia social, esses programas autônomos podem executar contas para espalhar conteúdo sem envolvimento humano."

[15] Ver Anexo A (p. 135) sobre contas removidas por país pelo Facebook e Twitter entre janeiro de 2019 e novembro de 2020 por estarem supostamente envolvidas com campanhas de desinformação.

A seguir o Quadro 5 apresenta uma organização das informações dispostas nesta subseção sobre os diferentes órgãos e instituições analisados.

Quadro 5 – Instituições russas identificadas e suas capacidades cibernéticas

Órgão/Entidade	Categoria	Envolvimento
FSB	Órgão do Estado (Segurança interna)	• Operações cibernéticas; • Suposta colaboração com grupos organizados da sociedade civil e crime organizado.
GRU	Órgão do Estado (Inteligência militar)	• Operações cibernéticas; • Operações de informação.
API	Instituição privada	• Operações de informação; • Atuação em redes sociais (Facebook, Twitter, etc).
RT	Instituição pública (Mídia de informação)	• Operações de informação; • Atuação em *website* próprio e redes sociais (além de canal de televisão)

Fonte: Elaborado com base em Connel e Vogler (2017), Giles (2016a), Giles (2016b), Soldatov e Borogan (2016), Mueller (2019) e Sidorenko (2016).

3.4.2 A Guerra Híbrida

O conceito operacional de guerra da Rússia é constituído por métodos e dinâmicas que buscam "influenciar a percepção e o comportamento do inimigo, da população e da comunidade internacional em todos os níveis" (SELHORST, 2016, p. 151, tradução própria).

No entanto, o componente cibernético não é utilizado de forma isolada para a concretização desses objetivos em muitos dos casos. Para isso são também empreendidos outros meios não cinéticos - como a pressão diplomática e econômica – e cinéticos, com a utilização das capacidades militares convencionais russas. A integração e articulação entre os componentes cinéticos e não cinéticos na estratégia russa é o que alguns teóricos chamam de GH.

O artifício ao uso de métodos não militares para a resolução de questões políticas sem o recurso único à violência, tem como pressuposto o que foi mostrado por Reed (2008) e Liang e Xiangsui (2002) no Capítulo 2, isto é, a percepção de que, com o desenvolvimento e difusão das soluções de TIC e com a imersão das atividades da sociedade no meio digital, novas capacidades para exercer influência e coerção surgiram, sendo a guerra de informação um conceito central nesse sentido. A nova realidade alterou a estratégia da conquista por meios violentos para a de controle por fatores externos e, nessa perspectiva, Bartosh (2018) defende que as soluções de TIC são as principais responsáveis por tornar possível o recurso ao controle externo de um país sem a obrigatória utilização de forças militares.

Nesse sentido, conforme explica o Coronel Bartosh (2018):

> nas condições modernas, a guerra não precisa estar associada à eclosão das hostilidades – a continuação da política pode ser realizada pela força, não apenas pelos militares, mas também por meios não militares (BARTOSH, 2018, não paginado, tradução própria).

Contudo, a Rússia não abandona a relevância das forças militares, versando que os recursos militares continuam sendo centrais para a consecução de objetivos políticos por meio da guerra, o que demonstra que a compreensão geral do país em relação aos conflitos é a de adoção de um modelo estratégico híbrido, em que instrumentos militares e não militares são combinados e integrados de acordo com a diversidade do cenário que deva ser enfrentado (BARTOSH, 2018).

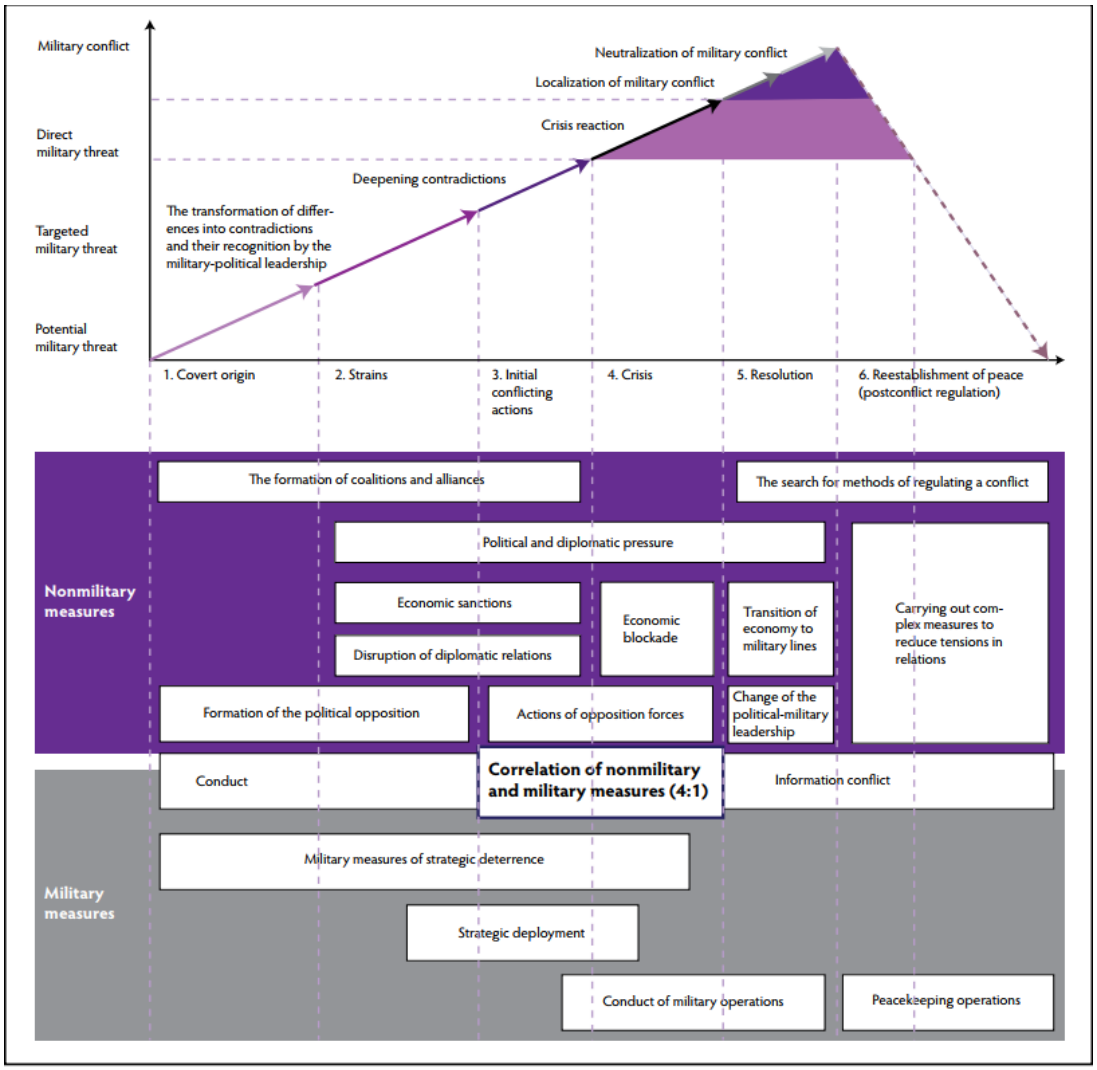
Apesar de não haver um consenso na bibliografia militar sobre a definição de GH, o coronel Bartosh apresenta a sua conceituação, defendendo que o termo “híbrida” se refere às mudanças na natureza das guerras, as quais passam a ocorrer em uma quantidade diversa de domínios – incluindo o cibernético – e de forma multidimensional, ou seja, abrangem uma combinação de instrumentos, dentre eles, o próprio componente militar convencional, mas também instrumentos de influência como os meios diplomáticos, informacionais, econômicos, regulatórios, técnicos, psicológicos, ideológicos e humanitários, por exemplo (BARTOSH, 2018).

A utilização de meios não militares como parte da atividade bélica, nos termos da GH apresentada por Bartosh (2018), contribui para que haja uma diminuição da fronteira perceptível entre os tempos tidos como de paz e os entendidos como de guerra, uma vez que, ainda que não haja enfrentamento violento durante todo o tempo, o clima constante de confrontação interestatal a partir do emprego de instrumentos não cinéticos, reflete um ambiente de tensão nas relações internacionais. Desse modo, busca-se o enfraquecimento e a derrota do inimigo a partir das diferentes frentes: militares, econômicas, informacionais e diplomáticas.

Por sua vez, o General Gerasimov, apesar de não fazer alusão direta ao termo GH, descreve o contexto atual dos conflitos como sendo significativamente caracterizados pelo emprego de métodos assimétricos e por ações indiretas. Nessa perspectiva, Gerasimov (2013) se aproxima da visão de GH descrita pelo coronel Bartosh (2018), o qual também ressalta a relevância do aspecto assimétrico representado pelos instrumentos não militares, como os recursos cibernéticos.

Abaixo, a Figura 8 apresenta o conceitual operacional de guerra compreendido pela Rússia, segundo a visão de Gerasimov (2013).

Figura 8 – Conceito operacional de guerra na concepção russa



Fonte: Bartles (2016).

Conforme expõe a Figura 8, Gerasimov (2013) divide os conflitos em seis fases ou estágios: origem oculta, escalada, eclosão de atividades conflitivas, crise, resolução e reestabelecimento da paz. O emprego gradual de meios não militares, bem como a perenidade do emprego de guerra de informação e a diferença de proporcionalidade entre o uso dos meios não militares e os meios militares, demonstram como o conceito operacional de conflito, de acordo com a concepção russa, fundamenta-se no método do 'controle reflexivo' (SELHORST, 2016; GILES, 2016b).

Em termos práticos o método do controle reflexivo se baseia em táticas que buscam influenciar a tomada de decisão do inimigo, fazendo-o optar por uma linha de ação que seja prejudicial aos seus próprios interesses nacionais ou que, no mínimo, seja favorável aos interesses nacionais russos. A forma de influenciar a decisão do inimigo passa por fornecer a ela uma série de informações que fundamentem a percepção que ele tem do ambiente, limitando o número de opções e direcionando a escolha (GILES, 2016a). Isso deve ser realizado durante todo o processo de tomada de decisão do inimigo, contaminando toda a cadeia decisória. Segundo Blandy (2009), isso pode ser alcançado:

> - Por meio da aplicação de pressão por força;
> - Por meio da influência na formulação da percepção da situação inicial na ótica do inimigo;
> - Moldando os objetivos do inimigo;
> - Moldando o algoritmo de tomada de decisão do inimigo;
> - Pela escolha do momento da tomada de decisão do inimigo (BLANDY, 2009, p. 2, tradução própria).

A função dos elementos cibernéticos nessa estratégia envolve essencialmente a propagação de fatos distorcidos ou politicamente enviesados, de modo a moldar de forma específica as impressões pessoais sobre determinados assuntos, conforme seja mais benéfico para a Rússia. Desse modo, Giles (2016a) mostra que:

> A Rússia procura influenciar a tomada de decisão estrangeira fornecendo informações poluídas, explorando o fato de que os representantes eleitos ocidentais recebem e são sensíveis aos mesmos fluxos de informações que seus eleitores. Quando a desinformação entregue dessa maneira faz parte da estrutura de decisões, isso constitui um sucesso para Moscou, porque um elemento-chave de controle reflexivo está em vigor (GILES, 2016b, p. 22, tradução própria).

Dessa maneira, por meio das suas capacidades cibernéticas, a Rússia cria um ambiente permissivo no território inimigo para o emprego das suas forças militares, minimizando a possibilidade de reações mais assertivas e garantindo o sucesso da operação.

Cabe ressaltar como o emprego dos recursos cibernéticos é um aspecto permanente no conceito operacional de conflito apresentado na Figura 8, o que corrobora com a concepção de que o elemento cibernético possui significativa relevância nos conjuntos de capacidades não militares para a condução da guerra, segundo a Rússia. É nesse sentido que Bartosh (2018) manifesta a necessidade de atenção para a crescente importância do elemento cibernético, identificando inclusive o seu potencial dissuasório:

> As enormes consequências destrutivas do uso de armas cibernéticas em uma guerra híbrida permitem hoje comparar a extensão de seu impacto nas forças armadas, na indústria, nos transportes e na população do país com os resultados do uso de armas nucleares. Isso sugere a necessidade de avançar a chamada dissuasão cibernética em pé de igualdade com a nuclear (BARTOSH, 2018, s/p, tradução própria).

É certo que há uma limitação do emprego militar nas campanhas externas, visto que o objetivo da Rússia, conforme mostrado ao longo desse capítulo, não é o de provocar um conflito em grande escala, mas sim agir a partir de uma retórica de defesa. Nesse sentido, conflagrar conflitos diretos e abertos com os EUA, individualmente, ou com a OTAN, como aliança, não são benéficos ao país do ponto de vista dos seus objetivos de política externa e, igualmente, da perspectiva racional e estratégica.

Portanto, apesar de no nível estratégico os recursos cibernéticos possuírem funções similares independentemente de qual seja o alvo, nos níveis tático e operacional surgem diferenças. O capítulo 4 explorará essas diferenças mostrando que o comportamento se altera conforme as características qualitativas, em termos de poder internacional, do alvo.

Os recursos cibernéticos russos podem também ser aplicados com o propósito de produzir efeitos desestabilizadores e subversivos sobre regimes políticos inimigos. De acordo com Giles (2016b) a estratégia russa de desestabilização e subversão de baseia no que ficou conhecido durante a Guerra Fria como medidas ativas. Elas seriam “uma série de técnicas evidentes ou encobertas para influenciar acontecimentos e comportamentos em, e ações de, outros países” (FIIA, 2016, p. 38, tradução própria). À época, as medidas ativas eram assimiladas como métodos de desestabilização e subversão orquestrados pela URSS contra instituições e sistemas de governo ocidentais, conforme um ex-oficial da KGB revelou em entrevista para a CNN em 1998:

> Não coleta de inteligência, mas subversão: medidas ativas para enfraquecer o Ocidente, para impulsionar as cunhas nas alianças da comunidade ocidental de todos os tipos, especialmente a OTAN, para semear discórdia entre aliados, para enfraquecer os Estados Unidos aos olhos do povo da Europa, Ásia , África, América Latina e, assim, preparar o terreno caso a guerra realmente ocorra. Para tornar a América mais vulnerável à raiva e desconfiança de outros povos (ARCHIVE.ORG, c2020, s/p, tradução própria).

A Rússia adaptou as medidas ativas para a era digital, buscando torná-las efetivas nos tempos atuais. Em termos gerais, o emprego das medidas ativas pela Rússia se fundamenta na utilização das mídias – tradicionais e de massa – para difundir desinformação sobre diversos assuntos, de modo a influenciar a população a adotar ideias e pautas que causem problemas para a coesão social e política das nações atingidas, buscando o enfraquecendo interno de seus adversários (THORNTON; MIRON, 2019). Desse modo, o Kremlin se empenha em apoiar a criação e a sustentação de veículos de mídia que propaguem desinformação ou reforcem narrativas favoráveis aos objetivos políticos russos, com a participação ativa e influente em mídias sociais (AJIR; VAILLIANT, 2018).

Por outro lado, efeitos desestabilizadores também podem ser obtidos por meio de ataques cibernéticos contra sistema informatizados que tenham presença cotidiana na vida da população, como a interrupção de sistemas bancários, financeiros, de transportes e trânsito, eleitorais, de comunicação, entre outros, conforme será abordado nos casos examinados no capítulo 4.

3.5 CONCLUSÕES PARCIAIS

O processo de análise realizado neste Capítulo buscou mostrar como as capacidades cibernéticas desenvolvidas pela Rússia cumprem um papel relevante para o alcance dos objetivos de política externa e da manutenção da segurança e defesa do país. Nesse sentido, partiu-se de uma abordagem que considerou as circunstâncias de política interna e a situação econômica da Rússia, inferindo que durante os governos Putin o país viveu uma relativa estabilidade nos assuntos internos, em muito devido ao ambiente econômico saudável e a centralização do poder em Moscou, possibilitada pela conjuntura russa no início do século XXI que contou também com o recrudescimento do autoritarismo.

A estabilidade no ambiente interno permitiu ao país perseguir uma política externa mais assertiva, baseada em um ideal de potência internacional que a Rússia deveria concretizar, com

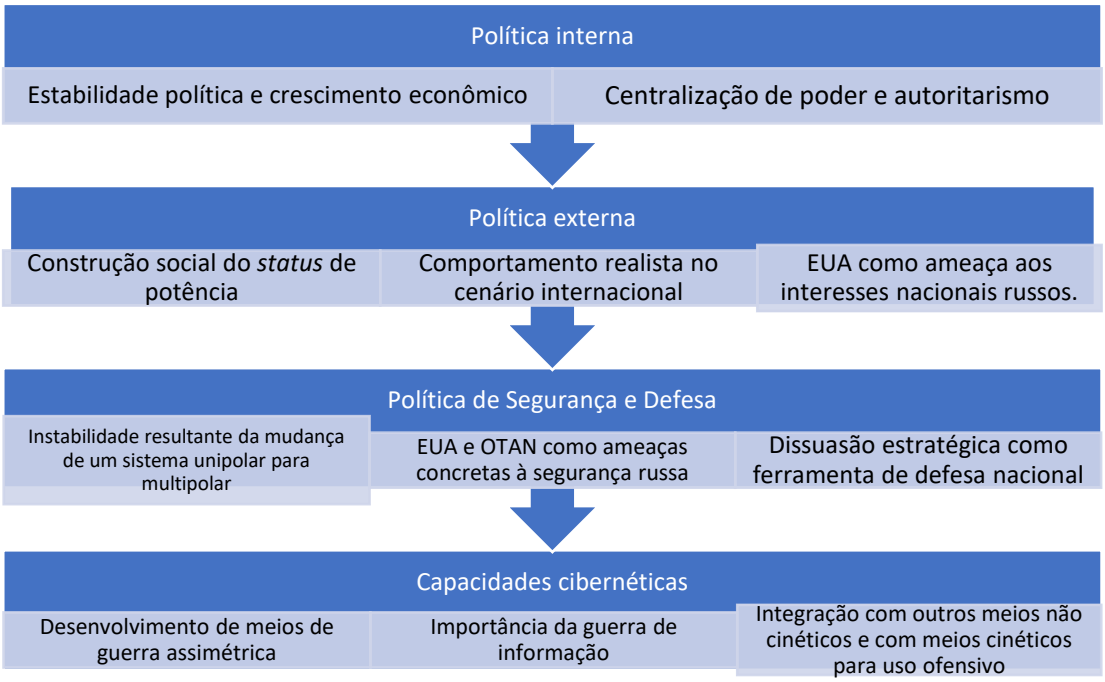
isso houve a elaboração de uma agenda internacional mais ampla, sem prejuízo do comportamento realista.

O retorno de contradições latentes com os posicionamentos e ações do Ocidente, recolocaram os EUA e a OTAN - a qual é considerada como uma ferramenta de política externa do primeiro - no centro da política de segurança nacional e defesa russa. As ações do Ocidente, na ótica russa, passam a serem vistas como ameaças à integridade do país e aos planos de projeção de poder internacional. Desse modo, a Rússia passa a vislumbrar a necessidade de desenvolver novas capacidades dissuasórias e de conflito, entendendo a inferioridade militar perante os EUA e a OTAN.

Nesse entorno, os recursos disponíveis no ciberespaço surgiram como uma fonte de capacidades assimétricas e de dissuasão para confrontar o Ocidente e como um importante artifício a ser usado de forma integrada com as forças convencionais, de modo a produzir resultados mais eficientes nas operações militares.

A Figura 9 apresenta de forma gráfica esse processo de análise, considerando os principais pontos observados.

Figura 9 – Processo de análise e constatações parciais



Fonte: Elaboração própria com base no conteúdo do Capítulo 3.

4 ANÁLISE DOS CASOS DE EXERCÍCIO DO PODER CIBERNÉTICO

O presente capítulo versa sobre os casos pré-selecionados para estudo empírico, conforme o apresentado na Introdução, de modo a cumprir com o último estágio do processo metodológico proposto. Dessa maneira, são tratados em ordem cronológica episódios nos quais a Rússia implementou estratégias que compreenderam o uso ofensivo de recursos cibernéticos.

Inicialmente é abordada a guerra cibernética contra a Estônia, no ano de 2007. Logo após, a Guerra Russo-Georgiana é colocada em perspectiva das CyberOps e InfoOps executadas pela Rússia, em benefício da atividade militar no âmbito operacional. Em seguida, a crise da Ucrânia é analisada, e novamente são frisados os aspectos relacionados aos recursos cibernéticos russos, nesse caso muito mais desenvolvidos e devidamente aprimorados, contando com poderosas armas cibernéticas e uma campanha de desinformação massiva e bem direcionada contra o país. Por fim, a interferência nas eleições dos EUA, demonstra o poder da Rússia em influenciar a política interna da maior potência do planeta através de uma organizada guerra de informação que conta com o auxílio de recursos cibernéticos sofisticados.

4.1 ESTÔNIA

4.1.1 Contexto

A relação da Estônia com a Rússia é antiga não apenas pela proximidade geográfica, mas principalmente pelo fato de o país báltico ter sido governado pelo Império Russo a partir do século XVIII e, posteriormente, ter sido ocupada pela URSS. Portanto, é notável que a Estônia, ao menos nos últimos séculos, esteve sob a órbita política da Rússia. O país somente se tornou independente de fato com a dissolução do bloco soviético em 1991 (CIA, 2021; VISITESTONIA, [201-?]).

Outrossim, um fator de importância para a contextualização dos acontecimentos descritos nesse subcapítulo é a admissão da Estônia na OTAN, em 2004 (OTAN, 2020). A entrada da Estônia na OTAN foi o resultado de um movimento gradual de aproximação com o Ocidente e, ao mesmo tempo, de tentativa de afastamento da área de influência da Rússia nos anos 90, quando o país

passava por conturbações políticas, sociais e econômicas, conforme foi demonstrado no Capítulo 3.

Uma característica relevante para a observação e exame das ações russas na Estônia concerne ao fato de que o Estado báltico é tido como um dos países mais digitalizados do mundo, levando em considerando o quantitativo de serviços públicos que são oferecidos de forma virtual, tendo também sido um destaque na época dos acontecimentos narrados no item Eventos. Atualmente, o país ocupa a terceira posição mundial no *E-Government Development Index* e a primeira posição no *E-Participation Index* (UN, 2020).

Segundo dados do portal e-Estonia, atualmente 70% dos cidadãos estonianos utilizam regularmente o ID-card, o documento de identificação digital do país. Além disso, cerca de 99% dos serviços estatais são prestados via *online*, o que é possível devido principalmente ao X-road, implementado em 2001 e considerado a espinha dorsal de todo o projeto de digitalização estoniano. Por meio do X-road os setores público e privado podem estabelecer a interligação entre seus sistemas, permitindo a distribuição de dados e informações de maneira rápida e ininterrupta (E-ESTONIA, 2020a)

O processo de digitalização dos serviços públicos na Estônia teve início nos anos 90, durante o período em que o governo federal adequava a burocracia pública, agora independente do aparato estatal soviético, ao mesmo tempo em que se via diante de uma situação fiscal deteriorada. Nesse sentido, a transposição dos serviços públicos para o ciberespaço foi enxergada como uma oportunidade para diminuir custos, concomitantemente com a vantagem de melhorar o atendimento ao público. No entanto, os desafios para a transformação do governo para a esfera digital eram consideráveis, uma vez que além da adequação dos serviços, o país precisava expandir o sinal e o acesso à Internet, ainda muito limitados naquela época (E-ESTONIA, 2020b).

Além dos investimentos em infraestrutura de telecomunicações e na área da tecnologia da informação, o processo de digitalização do país foi acompanhado de uma série de mudanças legislativas e regulatórias que modernizaram o ordenamento jurídico estoniano, possibilitando a implantação dos serviços públicos digitais (E-ESTONIA, 2020b).

O projeto de digitalização do governo também envolveu e ainda envolve os serviços policiais, de emergência pública, de saúde, entre outros. Ademais, a estratégia de digitalização do governo, por consequência do ambiente propício, motivou também a digitalização de muitos serviços privados, especialmente os bancários e financeiros (E-ESTONIA, 2020c).

Portanto, a Estônia é um país substancialmente dependente do ciberespaço para funcionar corretamente. As rotinas dos cidadãos, empresas e indústrias e, por fim, do governo, estão atreladas à uma série de serviços que são conectados à Internet. Contudo, não coincidentemente a Estônia foi e ainda é um exemplo eficaz para se dimensionar os efeitos de ataques cibernéticos para a sociedade, a economia e a segurança de um país.

As explicações para os ataques cibernéticos orquestrados pela Rússia contra a Estônia residem na relação histórica entre os dois países, no contexto da influência russa em seu entorno estratégico, na política de expansão da OTAN e na defesa das minorias étnicas e falantes russas na Estônia. Porém, a ação que serviu para que os ataques cibernéticos tivessem início foi a decisão, por parte das autoridades estonianas, de deslocar o monumento em homenagem aos soldados soviéticos de uma região central para uma região periférica em Tallinn, capital da Estônia (HERZOG, 2011; GREENBERG, 2019).

O aumento de tensões e o acirramento entre a minoria étnica e falante russa, que no geral defendia uma maior aproximação com a Rússia, e outra parcela da população que era mais favorável ao aprofundamento do relacionamento com as estruturas de governança ocidentais, resultou em confrontos nas ruas estonianas ao final do mês de abril de 2007, momento em que o monumento era removido da região central de Tallinn (HERZOG, 2011; GREENBERG, 2019).

4.1.2 Eventos

A decisão pelo deslocamento do monumento deu início aos enfrentamentos físicos entre indivíduos de etnia russa e de estonianos no dia 27 de abril de 2007, o mesmo dia em que os primeiros ataques cibernéticos foram registrados. No geral, a principal técnica utilizada para deixar os serviços de internet na Estônia *off-line* foram os ataques DDoS, um tipo de ataque cibernético considerado rudimentar, porém com efeitos importantes se realizado em larga escala e de forma coordenada, o que ocorreu no caso da Estônia (HERZOG, 2011; CONNEL; VOGLER, 2017).

Enquanto os ataques afetavam diferentes *websites* no país, além de serviços públicos e privados, dado o elevado tráfego de solicitações de acesso que tornavam os servidores que hospedavam os serviços indisponíveis, o governo estoniano já acusava o governo russo de estar por trás dos ataques. Contudo, o que dificultava a atribuição das investidas contra as infraestruturas de telecomunicações estonianas era que, ao menos em primeira análise, os ataques estavam vindo

de redes de computadores localizadas em diferentes países. Nesse momento o que se verificava, portanto, era a utilização de uma complexa *botnet* para gerar o congestionamento do tráfego de rede na Estônia e colocar o país *off-line* (CONNEL; VOGLER, 2017).

Com parcela considerável dos serviços pela internet parcial ou totalmente afetados, a Estônia recebeu o auxílio de diversos Provedores de Serviço de Internet (da sigla em inglês, ISP – *Internet Service Providers*) e de organizações de cibersegurança ocidentais para identificar e bloquear o tráfego malicioso, o que paulatinamente conteve os ataques russos. Contudo, concomitantemente com as comemorações de 8 de maio na Rússia – data em que os russos celebram a vitória na Segunda Guerra Mundial – novos e robustos ataques foram iniciados contra a Estônia (GREENBERG, 2019).

Nessa segunda investida alguns novos recursos cibernéticos foram utilizados. Verificou-se, por exemplo, que diversos *websites* estonianos foram modificados e imagens que faziam alusão ao nazismo foram introduzidas, inclusive relacionando o então primeiro-ministro da Estônia com Adolf Hitler (GREENBERG, 2019). Os ataques DDoS também foram amplificados na segunda investida. Uma matéria do The Guardian (2007), publicada dias após a segunda investida, mostra que os principais alvos dos ataques foram:

- A presidência estoniana e o parlamento do país;
- A quase totalidade dos ministérios do governo do país;
- Partidos políticos;
- Três das seis maiores organizações de notícias do país;
- Dois dos maiores bancos;
- Empresas especializadas em comunicações (THE GUARDIAN, 2007).

Conforme mostra Herzog (2011), a Estônia foi paralisada por meio dos ataques DDoS:

> O único banco da Estônia a relatar suas perdas operacionais devido aos ataques estimou os prejuízos em cerca de US $ 1 milhão, e ademais, os ataques evitaram que transações com cartão de crédito e caixa eletrônico ocorressem por vários dias. Enquanto isso, os *hackers* desativaram o servidor de e-mail do parlamento e os recursos de TI de vários ministérios do governo, paralisando a capacidade do Estado de responder com eficácia. Durante a crise, o ex-assessor de cibersegurança da Casa Branca Howard Schmidt chegou a dizer: "A Estônia construiu seu futuro com base em um governo e uma economia de alta tecnologia, e eles basicamente caíram de joelhos por causa desses ataques" (HERZOG, 2011, p. 51-52, tradução própria).

Somando-se a isso, conforme reportam Connel e Vogler (2017), houve uma terceira investida ainda no mês de maio, na qual diversos *websites* foram hackeados e modificados, passando a exibir mensagens de cunho nacionalista russo. No entanto, no mesmo período os ataques cessaram abruptamente sem um aparente um motivo, dando fim aos eventos de 2007 na Estônia.

Blank (2017) sugere que as redes do crime organizado russo tenham sido envolvidas no ataque cibernético contra o país báltico, como forma de mitigar provas que levassem ao comprometimento direto de Moscou. Nesse contexto, a *Russian Business Network* (RBN), notadamente envolvida em crimes cibernéticos, é apontada como autora dos ataques contra a infraestrutura estoniana (BIZEUL, 2007; BLANK, 2017).

Giles (2011), por sua vez, também comenta sobre a relação entre o crime organizado russo e as organizações de Estado para a execução dos ataques contra a Estônia, sendo destacado nesse caso em específico o envolvimento entre a RBN e o 16° centro do FSB. Além disso, a omissão das autoridades policiais e judiciárias russas em investigar, identificar e processar judicialmente os envolvidos com os ataques na Estônia também serve como um indicativo da conivência de Moscou com grupos da sociedade civil que, mesmo atuando em agravo descumprimento da legislação penal russa, não foram punidos.

4.1.3 Conclusões

Uma série de considerações podem ser feitas sobre os ataques cibernéticos na Estônia. A primeira delas é que os eventos ocorridos no país báltico demonstraram ao mundo o poder dos recursos cibernéticos para produzirem resultados assimétricos, por meio da corrupção, destruição e mal funcionamento de infraestruturas críticas nacionais, causando além de prejuízos econômicos, medo e desconfiança por parte da população, riscos a segurança nacional e a incapacidade do Estado em reagir para proteger esses bens imediatamente. Tal acontecimento pode ser observado como uma mudança de paradigma, pois até então apenas ataques cinéticos produziam tais efeitos (GREENBERG, 2019; CONNEL; VOGLER, 2017).

Connel e Vogler (2017), Chivvis (2017), Timothy (2014), Klimburg (2011) e Giles (2011) são alguns dos autores que chamam a atenção para a estratégia russa de utilização de ciberataques

por procuração, como modo de diminuir as possibilidades de atribuição dessas ações às agências de inteligência russas, sendo evidenciada essa abordagem no caso da Estônia.

Nesse sentido a Rússia foi exitosa, porque conseguiu testar as suas capacidades cibernéticas, aprender com a experiência obtida e observar os efeitos gerados. Além disso, os desdobramentos político-militares também devem ser considerados, dado que o ataque não resultou em nenhuma represália simétrica por parte da OTAN, o que evidenciou aos russos a possibilidade de atacar países-membros da OTAN sem que haja o escalonamento do conflito com a reverberação em respostas cinéticas que seriam prejudiciais à Rússia (GREENBERG, 2019).

Connel e Vogler (2017) explicam que, por mais que no âmbito tático os ataques cibernéticos não tenham produzido muito efeitos na Estônia, na esfera estratégica essas demonstrações foram importantes:

> Elas demonstraram a utilidade do bloqueio cibernético como meio de coerção, especialmente quando empregado em conjunto com outras ferramentas políticas, econômicas e de informação (CONNEL; VOGLER, 2017, p. 16, tradução própria).

Segundo Blank (2017), as ações russas também produziram efeitos na percepção que os países bálticos têm da OTAN e da sua capacidade em protegê-los contra esse novo instrumento de fazer guerra. Igualmente, a Rússia projetou também a sua influência de modo coercitivo sobre a Estônia:

> Ao interromper e possivelmente perturbar o governo e a sociedade da Estônia e ao demonstrar a incapacidade da OTAN de proteger a Estônia contra essa nova forma de ataque, os ataques cibernéticos visavam obrigar a Estônia a considerar os interesses russos em suas políticas. Em outras palavras, tinha o objetivo clássico de Clausewitz de dobrar o inimigo à sua vontade, neste caso - à vontade da Rússia. Na Estônia, como talvez também no caso da Geórgia, o ataque pode ter refletido não apenas um esforço para corrigir o comportamento da Estônia ou influenciar sua orientação, mas também um desejo de puni-la e impedir outros de seguir o exemplo, tornando-a um exemplo dos riscos para quem desafia a Rússia (BLANK, 2017, p. 86, tradução própria).

Outrossim, a OTAN posteriormente buscou aprender com as lições produzidas pelos ataques cibernéticos na Estônia. Com isso, uma série de estudos foram e são conduzidos pela organização com vista a explorar como o ciberespaço pode ser utilizado para a guerra e em como desenvolver mecanismos para capacitar os países-membros na área de defesa cibernética. O maior resultado dessa iniciativa foi a criação do *NATO Cooperative Cyber Defence Centre of Excellence*, sediado, de forma simbólica, em Tallinn (GREENBERG, 2019, CONNEL; VOGLER, 2017).

4.2 GEÓRGIA

4.2.1 Contexto

A Geórgia possui importância estratégica para a Rússia, tendo em vista a sua localização na fronteira sudoeste russa, no sul do Cáucaso. Atualmente, a relevância estratégica e geopolítica do país se deve especialmente ao fato de a Geórgia servir como um território-tampão entre a Rússia e a Turquia - uma potência regional em ascensão – e por formar um corredor pelo qual o Ocidente tem acesso ao Mar Cáspio e ao centro da Ásia. Portanto, caso a Geórgia se tornasse membro da OTAN, a Rússia teria prejuízos estratégicos em sua fronteira sudoeste, bem como poderia enfrentar dificuldades operacionais no Mar Negro (NILSSON, 2018).

Do mesmo modo que foi relatado sobre o caso da Estônia, a Geórgia no início dos anos 2000 buscou maior aproximação com as instituições ocidentais, estabelecendo cooperação com a OTAN, objetivando se tornar membro da Aliança, e buscando acesso à comunidade europeia. A política de aproximação com o Ocidente foi resultado da ‘revolução das rosas’ (uma das revoluções coloridas) em 2003, que retirou do poder um governo pró-Rússia, assumindo em seguida como presidente Mikheil Saakashvili (2004-2013) (GOMES; ALVES, 2020; NILSSON, 2018).

Saakashvili adotou uma posição favorável ao alinhamento com o Ocidente e recrudesceu o nacionalismo georgiano com movimentos de contestação da autonomia da Abecásia e de maior pressão sobre a Ossétia do Sul, que faz parte do território da região administrativa de *Shida Kartli*. Tanto a Abecásia quanto a Ossétia do Sul são regiões que se consideram repúblicas autônomas com populações constituídas em parte por pessoas de etnia russa (GOMES; ALVES, 2020).

O governo de Saakashvili também interferiu nos interesses geopolíticos russos relativos ao gás, com a construção do gasoduto Baku–Tbilisi–Ceyhan (BTC), um empreendimento de aproximadamente 1.700 km de extensão, que liga respectivamente as capitais do Azerbaijão e da Geórgia ao porto da cidade de Ceyhan, na Turquia, com a finalidade de transportar o gás azeri por meio do Mar Mediterrâneo até os mercados europeus (GOMES; ALVES, 2020; SOCAR, 2020)

De acordo com Nilsson (2018) e Gomes e Alves (2020), a política de aproximação com a OTAN e a UE e a contestação da autonomia da Abecásia e da Ossétia do Sul no governo de Saakashvili foram as causas para a eclosão da Guerra Russo-Georgiana em agosto de 2008. No

conflito, conforme será mostrado, a Rússia implementou a estratégia de GH, empregando CyberOps, InfoOps e operações militares em larga escala.

4.2.2 Eventos

No início do mês de agosto de 2008 a Geórgia movimentou tropas em direção à Abecásia e à Ossétia do Sul após o que o país considerou como "provocação" a realização de exercícios militares da Rússia próximos a fronteira (GOMES; ALVES, 2020).

Antes das primeiras investidas armadas por parte da Rússia, ataques cibernéticos foram deferidos contra *websites* georgianos entre os dias 6 e 7 de agosto, por meio de *botnets* coordenadas por sistemas de comando e controle operados por redes do crime organizado russo. Em fóruns *online* como o "xaker.ru" e "stopgeorgia.ru" foram disponibilizadas ferramentas e tutoriais, bem como, uma lista de alvos indicados para que qualquer usuário pudesse participar dos ataques cibernéticos contra a Geórgia. Novamente, os ataques cibernéticos por procuração eram executados pela Rússia (GOMES; ALVES, 2020; BLANK, 2017).

Os alvos dos ataques DDoS eram variados e incluíam entidades do setor público e privado georgiano, além de representações diplomáticas estrangeiras, de acordo com o que disserta Greenberg (2019):

> Essa guerra chegou em 7 de agosto. Um dia depois, uma onda quase simultânea de ataques distribuídos de negação de serviço atingiu trinta e oito sites, incluindo o Ministério das Relações Exteriores, o Banco Nacional da Geórgia, o parlamento, a corte suprema, as embaixadas dos EUA e do Reino Unido em Tbilisi e, novamente, o site do presidente Saakashvili. Como na Estônia, hackers desfiguraram alguns sites para postar fotos de Saakashvili ao lado de fotos de Hitler. E os ataques pareciam ser coordenados de forma centralizada: eles começaram com meia hora um do outro e continuariam inabaláveis até pouco depois do meio-dia de 11 de agosto, quando a Rússia estava começando a negociar um cessar-fogo (GREENBERG, 2019, p. 106, tradução própria).

Ainda no dia 7 de agosto, a Rússia deu início a invasão da Geórgia, empregando ataques militares, acompanhados de novas CyberOps e InfoOps, como mostra Nilsson (2018):

> As ações militares da Rússia foram acompanhadas por ataques cibernéticos contra os meios de comunicação do governo georgiano e contra a mídia georgiana, um influxo de mercenários e "voluntários" na Abkházia e na Ossétia do Sul e uma campanha internacional de desinformação alegando que o ataque inicial georgiano matou 2.000 ossétia do sul civis, acusação que justificou uma "intervenção humanitária" da Rússia (NILSSON, 2018, p. 24, tradução própria).

As CyberOps foram devidamente implementadas para dar suporte às operações militares russas e buscar maior vantagem no terreno, como mostra Blank (2017):

> Depois que as tropas russas estabeleceram posições na Geórgia, a lista de ataque se expandiu para incluir muitos mais sites de agências governamentais, instituições financeiras, grupos empresariais, instituições educacionais, mídia de notícias e um fórum de hackers georgiano para impedir qualquer resposta eficaz ou organizada à presença russa e induzir incerteza quanto ao que as forças de Moscou poderiam fazer [...] o objetivo claro dos ataques cibernéticos era apoiar e promover os objetivos das operações militares russas, já que foram programadas para começar em grande escala horas após o primeiro ataque militar russo. Os ataques terminaram logo após essas operações (BLANK, 2017, p. 90, tradução própria).

Apesar do aparente imediatismo do conflito, Blank (2017) disserta que os militares russos arquitetaram a guerra contra a Geórgia com certa antecedência, inclusive do ponto de vista cibernético. O autor argumenta que os russos estudaram a rede de internet da Geórgia anos antes do conflito eclodir, de maneira a já estabelecerem o modo de ataque e os seus alvos.

Conforme as tropas russas iam progredindo no território georgiano, os ataques cibernéticos eram ampliados e direcionados para os locais que seriam alvo dos ataques militares russos em seguida, como mostram Connel e Vogler (2017):

> [...] os ataques também foram alinhados geograficamente com as operações convencionais russas. Por exemplo, hackers russos atacaram sites do governo na cidade de Gori, no leste da Geórgia, junto com sites de notícias, pouco antes dos ataques aéreos russos à cidade (CONNEL; VOGLER, 2017, p. 18, tradução própria).

Enquanto os ataques cibernéticos auxiliavam o avanço das forças terrestres e se antecipavam aos bombardeios da força aérea russa, a marinha estabelecia, de forma bem sucedida, o bloqueio naval da Geórgia no Mar Negro. Por outro lado, as comunicações entre a Geórgia e o resto do mundo eram interrompidas pelos ataques cibernéticos, o que limitava as informações que os demais países tinham sobre o conflito às mídias de notícias russas, notadamente a *Russia Today* (atual RT) que transmitia as informações em inglês diretamente da Geórgia. A narrativa propagandeada pelas mídias russas buscava legitimar a ação das forças armadas do país, acusando o governo georgiano de violação da autonomia das regiões e de crimes contra as populações civis da Abecásia e da Ossétia do Sul e das forças de paz estacionadas nessas regiões (GOMES; ALVES, 2020).

No dia 12 de agosto a Rússia e a Geórgia estabeleceram um cessar-fogo, contudo, algumas divisões blindadas russas ainda avançaram no território georgiano até finalmente recuarem. No

entanto, a Rússia jamais retirou as suas tropas dos territórios da Ossétia do Sul e da Abecásia, regiões hoje sob controle efetivo russo (GREENBERG, 2019).

4.2.3 Conclusões

Apesar de os ataques cibernéticos terem sido tecnicamente pouco sofisticados, consistindo em grande parte de DDoS, o que mais se depreende do caso da Geórgia é a utilização combinada de elementos cibernéticos e militares convencionais para a condução do conflito (CONNEL; VOGLER, 2017). Desse modo, conclui-se que houve uma coordenação bem sucedida entre as CyberOps e InfoOps e os comandos militares.

Tal coordenação mostrou-se eficaz no nível estratégico, com a neutralização de alvos-chave da sistemática da cadeia de comando decisória e militar da Geórgia (sistemas de informação e comunicação) e do caos gerado dentre a população civil visto a falta de informações sobre o que realmente estava ocorrendo no país. Nesse contexto, a Rússia conseguiu desgastar a capacidade georgiana em se organizar e se mobilizar para responder. Já no nível tático e operacional, os ataques cibernéticos beneficiaram as operações militares, por serem localizados e coordenados de acordo com o avanço das tropas russas (GOMES; ALVES, 2020; GREENBERG, 2019; CONNEL; VOGLER, 2017; BLANK, 2017).

Ademais, deve ser ressaltado o papel das InfoOps russas. O controle da narrativa sobre a guerra pelas mídias de informação suportadas pelo Kremlin beneficiou as operações militares na Geórgia, uma vez que o Ocidente assistia ao que ocorria a partir dessas fontes de informação, gerando certa demora para que as instituições europeias e a OTAN pudessem apurar diretamente as informações e pressionar a Rússia pelo fim do conflito (GOMES; ALVES, 2020; GREENBERG, 2019).

Em relação ao resultado geopolítico da guerra, a Rússia conseguiu impor a sua influência na região do Cáucaso, principalmente por meio da manutenção da Geórgia em uma espécie de conflito congelado, uma vez que até os dias atuais, segundo informações da CIA (2020a), cerca de 18% do território da Geórgia - ou cerca de 12.500 km^2 – é ocupado pela Rússia, consistindo nas regiões da Abecásia e da Ossétia do Sul. Abaixo, a Figura 10 apresenta o mapa da Geórgia, no qual é possível visualizar os territórios da Abecásia e da Ossétia do Sul sob ocupação russa.

Figura 10 – Mapa da Geórgia

Fonte: CIA (2020b).

A preservação de um estado de tensão na Geórgia, sob a pressão russa, também manteve o país afastado da oficialização da entrada na OTAN e na UE, o que pode ser considerado como um ganho estratégico da Rússia. Além disso, novamente o Kremlin pode testar os limites dos países e das instituições ocidentais em relação aos atos de agressão russa em sua vizinhança (nesse caso inclusive com a investida militar) o que mais uma vez se mostrou vantajoso ao país dada a inação desses atores em socorrer imediatamente Tbilisi (NILSSON, 2018; BLANK, 2017).

Ademais, a guerra com a Geórgia foi um aprendizado importante para que as forças armadas russas pudessem identificar e sanar algumas debilidades operacionais, de modo a melhorar o desempenho das tropas em campanhas futuras, como foi o caso da Ucrânia, tratado na sequência. Da mesma forma, foi evidenciado o resultado dos investimentos realizados nas capacidades cibernéticas e de informação russas (CONNEL; VOGLER, 2017; BLANK, 2017).

Por fim, a influência da Rússia sobre a Geórgia permanece atrelada ao medo desse último perante a superioridade militar do primeiro. No entanto, a Rússia possui também ao seu dispor os elementos informacionais que servem aos seus interesses do país, segundo Nilsson (2018):

> A imagem que a Rússia busca projetar na Geórgia não é a de um vizinho amigo, mas de um vizinho poderoso e potencialmente implacável que não deve ser provocado. Resta saber por quanto tempo a Rússia permanecerá satisfeita com suas abordagens atuais e relativamente discretas em relação à Geórgia, especialmente porque os rebaixamentos em seus compromissos na Síria e na Ucrânia permitem prestar atenção em outros lugares (NILSSON, 2018, p. 55, tradução própria).

4.3 UCRÂNIA

4.3.1 Contexto

Assim como já relatado nos casos da Estônia e da Geórgia, a interferência da Rússia na Ucrânia esteve pautada na tentativa do afastamento da influência ocidental no entorno estratégico russo, de modo a evitar ameaças à segurança nacional e reforçar a manutenção da influência de Moscou na região. Nessa perspectiva, os eventos que se iniciaram no ano de 2014 foram resultados de anos de conturbações políticas internas na Ucrânia, ligadas principalmente à figura de Viktor Yanukovych e o seu papel político no relacionamento do país com a Rússia (BLANK, 2017).

Nas eleições presidenciais de 2004, Yanukovych disputou o cargo com Viktor Yuschenko, sendo este último um defensor do alinhamento ucraniano com as potências ocidentais. Yanukovych foi declarado eleito naquele ano, no entanto, por pressão popular devido às alegações de fraude nas eleições, Yanukovych acabou deixando o cargo e Yuschenko assumiu a presidência (BRITANNICA, 201-?).

Tal acontecimento repercutiu internacionalmente, sendo chamada de “revolução laranja”, em referência a cor das vestimentas dos apoiadores de Yuschcnko que participaram dos protestos. Para Moscou, esse movimento foi mais uma das chamadas “revoluções coloridas” que contavam com o apoio e articulação das potências ocidentais, especialmente dos EUA (BLANK, 2017).

Após uma presidência atribulada de Yuschenko e marcada por crises com a Rússia em relação aos gasodutos que abastecem a Ucrânia e boa parte da Europa ocidental, Victor Yanukovych, é eleito na eleição presidencial seguinte e assume o executivo da Ucrânia em 2010. Com Yanukovych no comando do país, a Rússia restaurou parte de sua influência política no governo ucraniano, enquanto a sociedade se dividia entre um maior alinhamento com a UE ou com a Rússia. No entanto, uma série de escândalos de corrupção no governo e a falta de uma melhor relação com a UE começaram a causar novos descontentamentos na sociedade (BRITANNICA, [201-?]).

Aliado ao ambiente de polarização sobre a postura de política externa que Yanukovych deveria seguir, recaiu também sobre o presidente e sua administração uma série de denúncias de corrupção, gerando importantes abalos na popularidade e no apoio político de Yanukovych. O estopim da crise política ocorreu quando nas vésperas de a Ucrânia oficializar o Acordo de

Associação UE-Ucrânia, o presidente ucraniano postergou a assinatura, o que foi visto por parcela da população como um gesto de aproximação com a Rússia em detrimento da UE (SHVEDA; HO PARK, 2016).

Uma série de protestos foram convocados nas ruas de Kiev para pressionar pela reversão da política adotada por Yanukovych. Houve uma rápida escalada de violência, com a polícia utilizando munições letais e empregando franco atiradores contra os manifestantes. Nesse cenário, durante dias, os manifestantes e a polícia se enfrentaram em Kiev nas proximidades da sede do governo ucraniano, com a concentração dos protestantes se estabelecendo na Maidan Nezalezhnosti (Praça da Independência, em ucraniano), o que denominou esses protestos de 'EuroMaidan'[16] (SHVEDA; HO PARK, 2016).

Os confrontos foram se intensificando e a pressão internacional foi crescendo, inclusive por meio da mobilização de pessoas por meio das redes sociais, como o Twitter, em que a hashtag EuroMaidan estava entre os assuntos mais comentados. A violência estava deixando muitos mortos e feridos, principalmente entre os manifestantes, mas também entre as forças de segurança. Com o clima de caos social e a pressão da população, o parlamento ucraniano retirou Yanukovych da presidência em fevereiro de 2014. Esse movimento ficou conhecido como Revolução da Dignidade (SHVEDA; HO PARK, 2016).

A Rússia vislumbrou nesse novo contexto político ucraniano, que era marcado por um sentimento nacionalista e pró-Ocidente, um perigo real à influência histórica russa sobre o país e aos povos falantes russos na Ucrânia, dada a aparente violência dos movimentos, e a possibilidade de a Ucrânia vir a fazer parte da OTAN, fazendo com a aliança militar estivesse novamente na fronteira com o território russo. Ademais, a possibilidade de a Ucrânia se estabelecer sob o guarda-chuva de instituições ocidentais sinalizava uma ameaça em potencial para os ativos estratégicos russos localizados no país, com destaque para a base principal da Frota do Mar Negro da marinha russa, estabelecida na cidade de Sevastopol, península da Criméia (SELHORST, 2017).

[16] A simbologia do nome da praça é importante para compreender os protestos que culminaram na Revolução da Dignidade.

4.3.2 Eventos

No ciberespaço a reação russa iniciou antes mesmo da derrubada do governo de Yanukovych, mas ganhou impulso com o resultado dos protestos de "EuroMaidan" e, principalmente, após a tomada e anexação da Crimeia. Nessa perspectiva, de acordo com com Jaitner e Mattsson (2015):

> Quando a crise da Ucrânia atingiu seu primeiro pico com a anexação da península da Crimeia, ficou claro que a Rússia estava conduzindo intensas Operações de Informação (OIs) e, mais ainda, que estava obtendo sucesso com elas. A Guerra de Informação (GI) como tal, entretanto, começou muito antes e ganhou intensidade desde a primeira demonstração Euromaidan (JAITNER; MATTSSON, 2015, p. 40, tradução própria).

Portanto, as abordagens que se destacam no contexto dos recursos cibernéticos russos, no caso da crise ucraniana, são os relativas às InfoOps, operacionalizadas tanto pela mídia formal russa quanto por *trolls* e *bots* que espalhavam nas redes sociais e blogs na internet informações falsas e/ou enviesadas que buscavam relacionar grupos nacionalistas e extremistas ucranianos com o governo constituído em Kiev (GRAPHIKA, 2020; JAITNER; MATSSON, 2015; CONNEL; VOGLER, 2017).

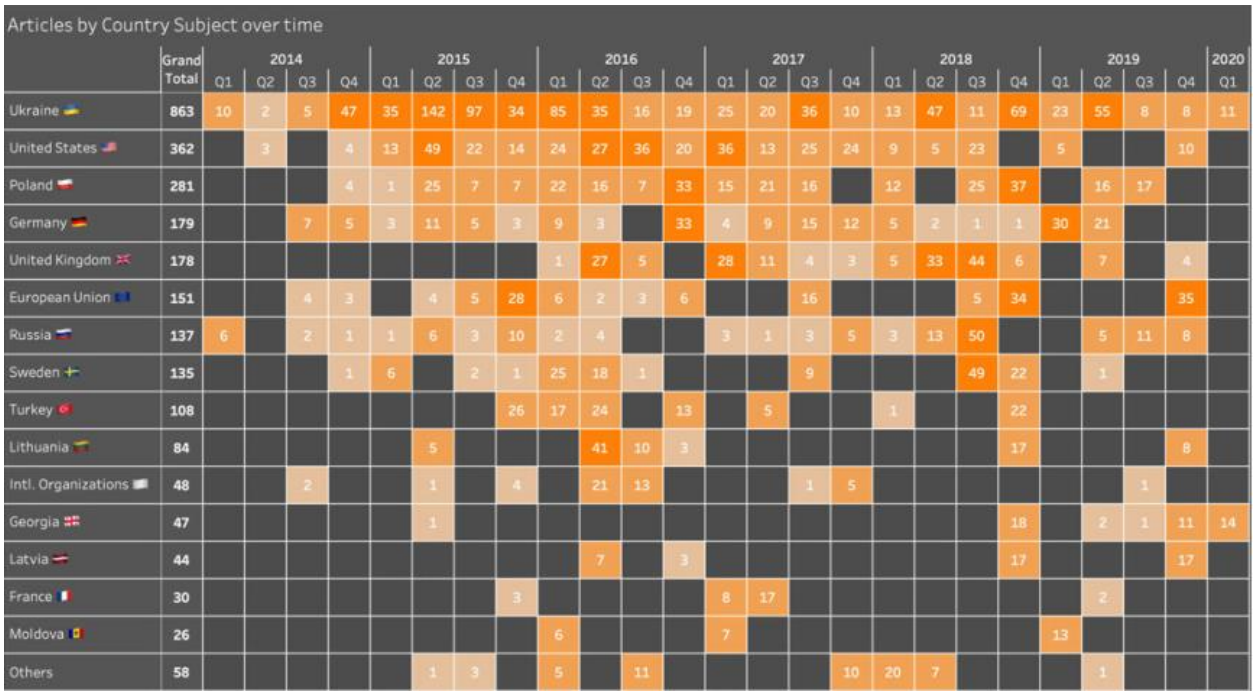
Imagens e supostos relatos de refugiados ucranianos que se dirigiam à Rússia eram divulgados pela internet e chegavam até a opinião pública ocidental, procurando influenciar também os governos europeus a se afastarem de Kiev. Constantemente notícias veiculadas especialmente pela RT colocavam dúvidas na idoneidade do governo ucraniano, dentre acusações sobre ideais nazifascistas até a fragilidade das instituições ucranianas e da segurança em torno da manutenção da governança e controle do país pelo governo (RUSNÁKOVÁ, 2017).

A participação de organizações como o *Pravy Sektor* e o *Spilna Spraya* nos protestos de EuroMaidan reforçaram a narrativa da Rússia de que o governo ucraniano estaria alinhado aos ideais extremistas e nacionalistas desses movimentos (RITTER, 2017).

Um relatório da firma de análise de dados de mídias e redes sociais Graphika (2020), nomeou as campanhas de desinformação russa na internet como operação "Secondary Infektion", em alusão às InfoOps soviéticas das décadas de 70 e 80, denominadas de operação "Infektion". O documento apresenta, por meio de dados, como a Rússia teria supostamente utilizado as redes sociais e blogs na internet para espalhar notícias e narrativas falsas ou enviesadas por meio de *trolls* e *bots*, procurando confundir a opinião pública e causar instabilidade social e política em diversos países, dentre eles a Ucrânia.

Abaixo, a Figura 11 evidencia os países que mais foram alvo das InfoOps russas, de acordo com o estudo da Graphika (2020).

Figura 11 – Países mais atingidos pelas operações de informação russas entre 2014 e 2020[17]



	Grand Total	2014				2015				2016				2017				2018				2019				2020
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1
Ukraine	863	10	2	5	47	35	142	97	34	85	35	16	19	25	20	36	10	13	47	11	69	23	55	8	8	11
United States	362		3		4	13	49	22	14	24	27	36	20	36	13	25	24	9	5	23		5			10	
Poland	281				4	1	25	7	7	22	16	7	33	15	21	16		12		25	37		16	17		
Germany	179			7	5	3	11	5	3	9	3		33	4	9	15	12	5	2	1	1	30	21			
United Kingdom	178									1	27	5		28	11	4	3	5	33	44	6		7		4	
European Union	151			4	3		4	5	28	6	2	3	6			16				5	34				35	
Russia	137	6		2	1	1	6	3	10	2	4			3	1	3	5	3	13	50			5	11	8	
Sweden	135				1	6		2	1	25	18	1				9				49	22		1			
Turkey	108								26	17	24		13		5			1			22					
Lithuania	84						5				41	10	3								17				8	
Intl. Organizations	48			2			1		4		21	13				1	5							1		
Georgia	47						1														18		2	1	11	14
Latvia	44										7		3								17				17	
France	30								3					8	17								2			
Moldova	26									6				7								13				
Others	58						1	3		5		11					10	20	7				1			

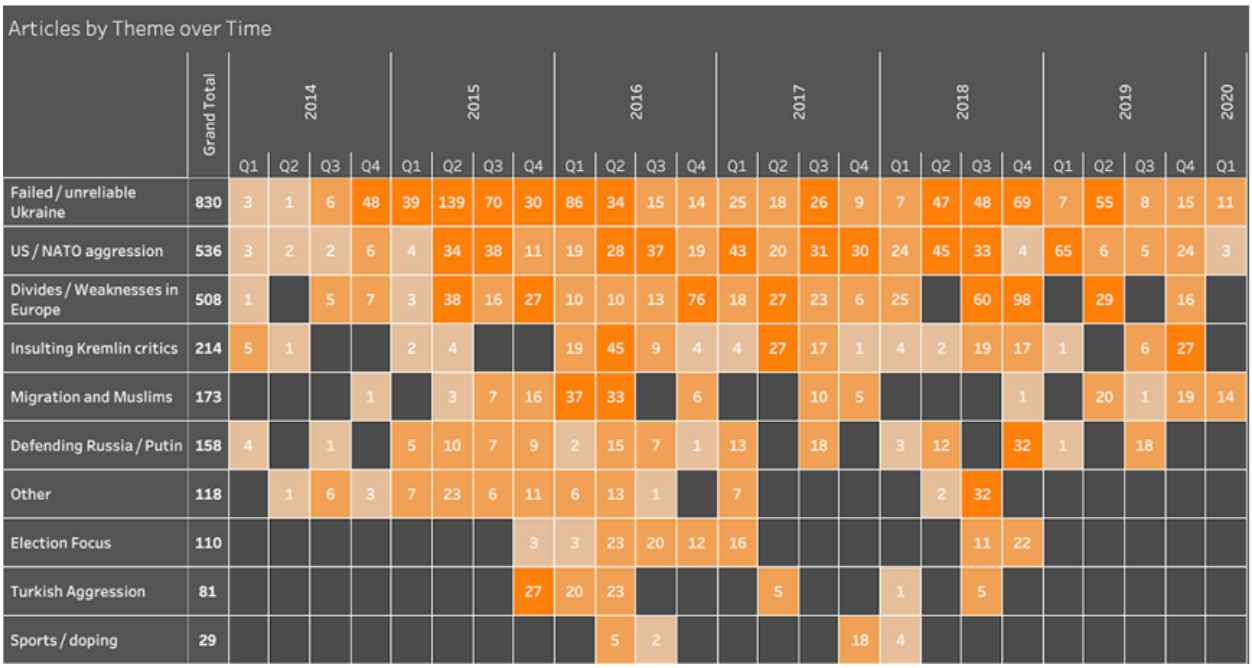
Fonte: Graphika (2020).

Conforme pode ser notado, a Ucrânia foi o país mais atingido pelos conteúdos de desinformação propagados pela campanha russa, de acordo com o mapeamento realizado. O período com maior quantidade de artigos postados nas redes sociais que buscavam atacar a Ucrânia e seu governo foi entre o final de 2014, todo o ano de 2015, até meados de 2016, coincidindo com as épocas mais conflitivas da crise ucraniana, como por exemplo as batalhas nas regiões de Luhansk e Donetsk entre forças ucranianas e grupos separatistas pró-Rússia, apoiados por Moscou (GRAPHIKA, 2020).

A seguir, a Figura 12 apresenta os temas abordados e a quantidade de artigos sobre cada tema identificados e atribuídos às InfoOps russas desde 2014 até o primeiro trimestre de 2020.

[17] Quantitativo de postagens identificadas e atribuídas às contas inautênticas por trimestre.

Figura 12 – Temas e frequências das operações de informação russas desde 2014[18]



Articles by Theme over Time

	Grand Total	2014				2015				2016				2017				2018				2019				2020
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1
Failed / unreliable Ukraine	830	3	1	6	48	39	139	70	30	86	34	15	14	25	18	26	9	7	47	48	69	7	55	8	15	11
US / NATO aggression	536	3	2	2	6	4	34	38	11	19	28	37	19	43	20	31	30	24	45	33	4	65	6	5	24	3
Divides / Weaknesses in Europe	508	1		5	7	3	38	16	27	10	10	13	76	18	27	23	6	25		60	98		29		16	
Insulting Kremlin critics	214	5	1			2	4			19	45	9	4	4	27	17	1	4	2	19	17	1		6	27	
Migration and Muslims	173				1		3	7	16	37	33		6			10	5				1		20	1	19	14
Defending Russia / Putin	158	4		1		5	10	7	9	2	15	7	1	13		18		3	12		32	1		18		
Other	118		1	6	3	7	23	6	11	6	13	1		7					2	32						
Election Focus	110								3	3	23	20	12	16						11	22					
Turkish Aggression	81								27	20	23				5			1		5						
Sports / doping	29										5	2					18	4								

Fonte: Graphika (2020).

Conforme mostra o relatório, todos os temas possuem uma relação com outros episódios relevantes:

> O exemplo mais marcante é a maneira como o Secondary Infektion repentinamente começou a atacar a Turquia depois que a Turquia abateu um jato russo: a queda aconteceu em 25 de novembro de 2015, e o primeiro ataque do Secondary Infektion na Turquia veio apenas uma semana depois, em 1º de dezembro. Mas outros temas também combinavam com as narrativas do Kremlin: a representação da Ucrânia como um parceiro não confiável para o Ocidente, as acusações de que os Estados Unidos estavam interferindo nos ex-estados soviéticos e os ataques à Agência Mundial Antidoping e aos Jogos Olímpicos de Inverno de 2018 (dos quais A Rússia foi banida) todas coincidem de maneira única com as narrativas estratégicas da Rússia do período. Os ataques a figuras como Aleksei Navalny (Rússia), Mikheil Saakashvili (Geórgia), Jaroslaw Kaczynski (Polônia), Dalia Grybauskaite (Lituânia) e o grupo investigativo Bellingcat também são consistentes com uma atribuição a atores russos (GRAPHIKA, 2020, não paginado, tradução própria).

Nota-se, portanto, que a partir do início da crise ucraniana a Rússia colocou em prática uma ampla operação de informação que esteve - e provavelmente ainda está - ativa e à cargo da agenda política russa doméstica e internacional.

Conforme comentado anteriormente, a estratégia russa de guerra de informação na Ucrânia e para a Criméia, especialmente, se baseou nos vínculos históricos e étnicos da população ucraniana

[18] Quantitativo de postagens identificadas e atribuídas às contas inautênticas por trimestre.

para com a Rússia. Na península da Criméia, por exemplo, cerca de 58,5% da população é de etnia russa, o que contribuiu para que a propaganda do país fosse efetiva (RUSNÁKOVÁ, 2017). Conforme afirma Rusnáková (2017):

> O objetivo da guerra de informação russa na Crimeia era secretamente enganar, confundir, convencer e atrair a minoria de língua russa (que de fato constitui a maioria da população da península) que habita a península sem qualquer resistência ou uso de força, empregando a manipulação de informações de forma que seja benéfica para os objetivos políticos da Rússia, neste caso para evocar o surgimento de sentimentos pró-russos e, através disso, para legitimar suas ações ilegais - a anexação de território (RUSNÁKOVÁ, 2017, p. 359, tradução própria).

Observa-se, por conseguinte, que o ambiente psicológico e informacional da população ucraniana e até mesmo dos corpos militares do país estava constantemente sendo permeado por propagandas e campanhas de desinformação russas que contribuíram para que as atividades militares, particularmente na Criméia, fossem exitosas e sem confrontos em larga escala. Como mostra Selhorst (2017):

> A televisão e a Internet eram os meios de comunicação dominantes na Ucrânia. Na Crimeia, no total, 95% da população obtinha suas notícias nos canais de televisão, quase todos de propriedade estatal russa. Cerca de 50% da população da Crimeia obtinha suas notícias da Internet e 70% dos usuários da Internet da Crimeia contam com a coleta de notícias nas duas principais redes sociais russas disponíveis. Russos e ucranianos analisaram informações sobre os sentimentos coletados na Internet, encontrando uma pontuação de 76% para os sentimentos pró-russos na região. Na Rússia, esses números eram comparáveis; mais de 75% da população confia em sua mídia estatal. Os provedores de notícias independentes são avaliados com 30% de confiabilidade, e os provedores de notícias estrangeiros com apenas 5% de confiabilidade. (SELHORST, 2017, p. 160, tradução própria).

No entanto, as InfoOps não foram as únicas demonstrações da capacidade cibernética russa. Segundo Connel e Vogler (2017),

> Os *hackers* russos utilizaram *spear phishing*, *malware*, ataques DDoS, ataques de negação de serviço de telefonia (TDoS) e outras formas de ciberinterrupção e espionagem para conduzir uma ofensiva constante de ataques cibernéticos contra o governo da Ucrânia, militares, telecomunicações e a infraestrutura de tecnologia da informação do setor privado. Ataques cibernéticos têm sido usados para interromper as comunicações, obter e vazar documentos e planos do governo e desfigurar ou derrubar sites públicos e privados e sistemas de computador (CONNEL;VOGLER, 2017, p. 19, tradução própria).

O isolamento promovido pela interrupção das comunicação na Crimeia fez com que as tropas russas adentrassem o território da região e estabelecessem posições estratégicas, como os quartéis das forças ucranianas, polícias e da sede do governo local sem maiores dificuldades, dado o ambiente de confusão, de falta de informações e de coação prévia realizada por meio de

mensagens de direcionadas aos oficiais militares ucranianos lotados na Crimeia, para convencê-los para desertarem para o lado russo. Desse modo, e contando com forças militares uniformizadas sem insígnia ou qualquer outra identificação a Rússia conseguiu estabelecer rapidamente o controle da Crimeia (RUSNÁKOVÁ, 2017).

O episódio da Crimeia mostra como os elementos da guerra híbrida foram trabalhados e empregados de forma coordenada para o alcance do objetivo central: o controle da península de maneira rápida e eficaz. Jaitner e Mattsson (2015), evidenciam a presença desses instrumentos durante todo o processo de invasão e controle:

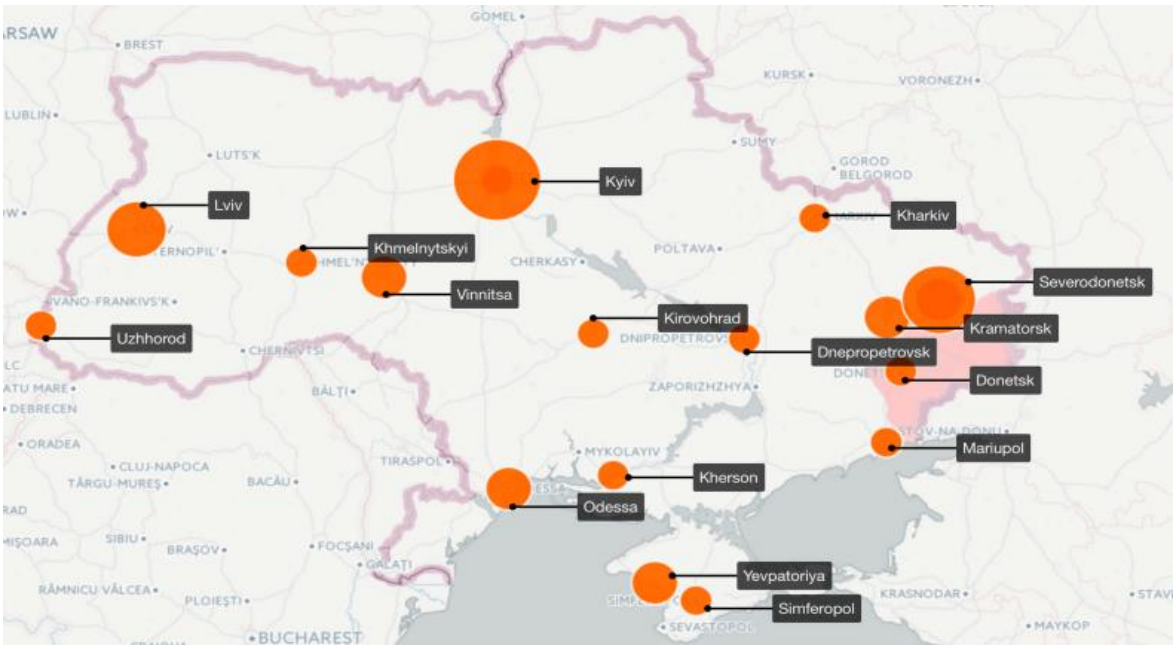
> Os eventos na Crimeia que aconteceram na primavera de 2014 fornecem pistas importantes para a interação entre IOs e atividade cinética. O curso dos acontecimentos - desde a tomada do parlamento em Simferopol e o desmantelamento da presença militar ucraniana na península, ao contestado referendo e à anexação de facto da área à Federação Russa - foi acompanhado por intensa atividade destinada a controlar o fluxo de informação. Esta atividade se estendeu por todo o espectro da comunicação e incluiu cinética, cibernética e IOs visando as camadas física, lógica e social da comunicação (JAITNER; MATTSSON, 2015, p. 45, tradução própria).

A firma de segurança cibernética *LookingGlass* em um de seus relatórios sobre os ataques cibernéticos identificou a presença de *malware* em computadores do governo ucraniano e das forças armadas do país, provavelmente para realizar ciberespionagem e beneficiar as operações militares russas na Ucrânia com as informações relativas às decisões políticas e militares de Kiev (LOOKINGGLASS, 2015).

A firma nomeou de *Operation Armageddon* a operação cibernética russa que infectou os computadores entre 2014 e 2015 e corroborou com as acusações realizadas pelas investigações conduzidas pelo Serviço de Segurança da Ucrânia (da sigla em ucraniano, SBU) em que foi atribuído ao 16º e ao 18º centros do FSB a responsabilidade pelos ataques (LOOKINGGLASS, 2015).

Abaixo, a Figura 13 exibe a localização no território ucraniano das principais cidades em que se identificou os ataques cibernéticos russos que infectaram os computadores para fins de ciberespionagem.

Figura 13 – Localização dos ataques cibernéticos identificados pela *LookingGlass*



Fonte: Lookingglass (2015).

Apesar de haver uma dispersão geográfica dos alvos, observa-se que as principais cidades atingidas foram a capital Kiev e as regiões próximas ao território sob disputa no leste ucraniano, marcado com a cor vermelho no mapa. Tal distribuição, em conjunto com as investigações que reconheceram o tipo de *malware* empregado e a autoria dos ataques, sugerem a possível utilização dos dados coletados para fins de inteligência militar.

Outro sinal da sofisticação das ações russas contra a Ucrânia no âmbito cibernético foi o ataque realizado contra a rede elétrica ucraniana em dezembro de 2015 que deixou uma parcela da população sem energia. Conforme relatam Connel e Vogler (2017):

> Usando acesso remoto para controlar e operar disjuntores, os invasores desligaram os centros de distribuição, causando quedas de energia que afetaram mais de 220.000 residentes ucranianos. Os ciberatores apagaram alguns sistemas executando o *malware* KillDisk na conclusão do ataque cibernético (CONNEL; VOGLER, 2017, p. 20, tradução própria).

Investigações posteriores sobre o ataque demonstraram que os atores planejaram e estudaram com antecedência as particularidades do sistema, bem como as credenciais de usuário necessárias para acessar o sistema SCADA que controlava a rede elétrica (ZETTER, 2016). Acredita-se também que os russos tenham invadido os computadores com o *malware*

BlackEnergy[19], um vírus do tipo *trojan* que é utilizado para monitorar, mapear e atacar os diversos componentes do sistema SCADA, incluindo também uma modificação que inclui uma *backdoor* no sistema para acesso permanente por parte dos atacantes (CONNEL; VOGLER, 2017).

Um relatório da firma de segurança cibernética *FireEye* sobre o ataque cibernético contra a rede elétrica ucraniana, em que foi detectada a existência do *BlackEnergy*, atribui a autoria ao grupo *hacker Sandworm*, o qual pertencente a unidade 74455 do GRU (FIREEYE, 2016; MUELLER, 2019).

Blank (2017) acredita que o ataque contra a rede elétrica ucraniana tenha sido uma reação à escalada do conflito por parte dos ucranianos, o que demandava uma resposta simétrica. A Ucrânia havia cortado os cabos que distribuíam eletricidade para a Crimeia, o que deixou a península sem energia até que a Rússia pudesse construir a infraestrutura necessária para abastecer a região com a energia vinda do território russo. Nesse caso, além da resposta, o ataque cibernético foi um recado claro das capacidades cibernéticas russas para Kiev.

Em contrapartida, Connel e Vogler (2017) consideram que acima de tudo, o ataque cibernético contra a rede elétrica buscou produzir efeitos psicológicos na população ucraniana, contribuindo para minar a confiança da opinião pública no governo de Kiev:

> Em termos gerais, a Rússia parece ter usado atividades cibernéticas secretas em coordenação com outras ferramentas de informação e operações militares para criar um ar geral de confusão e incerteza em relação à capacidade do governo ucraniano de proteger seus sistemas de informação, bem como a integridade de qualquer informação sendo comunicada. Por meio dessa campanha cibernética, a Rússia foi capaz de comprometer de maneira silenciosa e persistente a capacidade do governo e dos militares ucranianos de se comunicar e operar, minando assim a legitimidade e a autoridade das instituições políticas e militares ucranianas (CONNEL; VOGLER, 2017, p. 19, tradução própria).

4.3.3 Conclusões

A articulação entre os meios não-cinéticos e os meios militares foi exitosa ao ponto de permitir a invasão e o controle de uma área de 27.000 km^2 sem maiores resistências por parte do adversário. Esses resultados, como deve ser ressaltado, vão além da reestruturação das forças armadas russas, que teve início após 2010 e surtiram bons resultados na recuperação da qualidade

[19] Segundo reporta a firma de segurança cibernética Kaspersky, "BlackEnergy é um *trojan* usado para conduzir ataques DDoS, ciberespionagem e ataques de destruição de informações. [...] Desde meados de 2015, o grupo BlackEnergy APT tem usado ativamente e-mails de *spear-phishing* que contêm documentos Excel maliciosos com macros para infectar computadores em uma rede alvo (KASPERSKY, 2021, não paginado, tradução própria).

operacional militar russa, mas se devem especialmente a estratégia de guerra híbrida, com o emprego de CyberOps e InfoOps em larga escala (SELHORST, 2017).

A Figura 14 abaixo apresenta o mapa da Ucrânia, com destaque para a capital Kiev e as cidades de Luhansk e Donetsk, atualmente controladas por forças pró-russas e a península da Crimeia, anexada pela Rússia.

Figura 14 – Mapa da Ucrânia

Fonte: CIA (2020).

Os instrumentos da Rússia para implementar InfoOps foram expandidos e alcançaram as redes sociais e os blogs na internet, gerando efeitos psicológicos diretos sobre a opinião pública russa, ucraniana e internacional. O desenvolvimento das capacidades relacionadas às CyberOps também são um ponto a ser destacado: enquanto na Estônia e Geórgia essas operações eram praticamente limitadas aos ataques DDoS, menos sofisticados, no caso da Ucrânia o que se constatou foi o surgimento de *malwares* especialmente desenvolvidos para a infecção de determinados sistemas, implantados por meio de estratégias que se fundamentaram especialmente na engenharia social do *spear phishing* (CONNEL; VOGLER, 2017; BLANK, 2017).

No que concerne aos resultados políticos, a Rússia supostamente adotou a mesma estratégia da guerra contra a Geórgia: manter o país instável e em um conflito congelado para afastar a possibilidade de absorção por parte das organizações internacionais ocidentais, ao mesmo tempo em que a influência russa é conservada na região. De fato, as relações com a UE e com a OTAN

não se traduzem em acordos concretos de adesão à nenhuma dessas estruturas, ainda que exista cooperação no campo econômico e militar entre a Ucrânia e esses blocos.

Em compensação, o Ocidente agiu de forma mais assertiva contra a Rússia por meio de sanções econômicas contra as autoridades russas e alguns setores públicos e privados do país. No entanto, não houve nenhuma resposta militar e a Rússia mantém o controle da Crimeia e o apoio aos grupos separatistas nas regiões de Luhansk e Donetsk, fazendo com que o conflito perdure até os dias atuais.

4.4 EUA

4.4.1 Contexto

A eleição presidencial dos EUA de 2016 foi marcada por acusações de que a Rússia interferiu diretamente no resultado eleitoral, por meio de InfoOps e CyberOps que contribuíram para dividir a população estadunidense, minar a confiança no processo eleitoral e nas instituições de Estado do país (BAEZNER e ROBIN, 2017; USA, 2020).

Consoante ao que foi trabalhado no capítulo 3, na análise das políticas externa e de segurança e defesa da Rússia, os EUA foram retratados como o maior perigo ao país e aos seus interesses nacionais. Sugere-se, portanto, que a relação entre a Rússia e os EUA se deteriora gradativamente, ao menos com maior celeridade, desde as ações russas na Estônia e na Geórgia.

Ao passo que a Rússia já observava o suposto envolvimento dos EUA na deposição de governos e regimes até então aliados ao Kremlin desde o final dos anos 90 e início dos 2000, foi durante a eleição presidencial russa de 2011 que o país pela primeira vez acusou os EUA de terem buscado interferir na política interna russa (SHANE, 2017).

O governo russo acusa os serviços de inteligência americanos de terem incentivado e patrocinado os atos de protesto em diversas cidades russas nos dias em que antecederam a eleição que reconduziu à presidência russa o então primeiro-ministro Putin. Os protestos eram contrários a eleição de Putin e denunciavam supostas irregularidades no processo eleitoral que comprometeriam a sua integridade (GUTTERMAN; BRYANSKI, 2011).

No entanto, as motivações para as supostas interferências da Rússia na eleição presidencial dos EUA em 2016 vão além de uma simples reação ao caso de 2011. Enfraquecer internamente os EUA por meio do emprego de CyberOps e InfoOps se tornou uma oportunidade após os resultados positivos das campanhas russas anteriores (BAEZNER e ROBIN, 2017).

Em concordância com o que será mostrado, diferentemente dos casos da Geórgia e Ucrânia em que o emprego de forças militares era essencial para a concretização de determinados objetivos estratégicos e, ademais, era possível devido à proximidade geográfica dos territórios, o menor poder relativo desses Estados e a falta de alianças militares de importância. No presente caso os recursos cibernéticos russos foram utilizados com o objetivo central de desestabilizar a política interna americana (MUELLER, 2019; USA, 2020).

4.4.2 Eventos

As primeiras ações da Rússia antecedem em cerca de um ano a eleição presidencial de 2016, conforme expõem BAEZNER e ROBIN (2017):

> Desde 2015, várias instituições dos EUA e o Comitê Nacional Democrata dos EUA (DNC) foram vítimas de uma série de invasões em suas redes. Os perpetradores, que se acredita serem os grupos de hackers russos APT28 e APT29, usaram e-mails de *spear phishing* para entregar malware do tipo Ferramenta de Administração Remota. Essas técnicas permitiram que os grupos de *hackers* acessassem remotamente as redes de computadores de suas vítimas e obtivessem acesso a dados confidenciais. Os dados roubados do DNC foram publicados posteriormente em momentos estratégicos durante as eleições presidenciais dos EUA, interferindo no processo democrático e potencialmente ajudando o candidato republicano Donald Trump a vencer as eleições (BAEZNER; ROBIN, 2017, p. 4, tradução própria).

Como mostra a *FireEye* (2017), além da invasão da rede de computadores do DNC representar mais uma evolução das capacidades cibernéticas russas, as atividades realizadas demonstram que os elementos de guerra cibernética e guerra de informação se tornaram indissociáveis na estratégia russa. Nesse sentido, outros ataques cibernéticos contra alvos americanos também atribuídos à Rússia, como o do chefe de campanha de Hillary Clinton – a candidata democrata – e o Comitê de Campanha Democrata do Congresso (da sigla em inglês, DCCC), tiveram como resultado o vazamento de dados e informações.

Apesar de os atores aparentes dos ataques terem publicado muitas das informações e documentos, os principais vazamentos partiram de *websites* já conhecidos pela divulgação de

informações confidenciais de governos e empresas, como são os exemplos do WikiLeaks e DCleaks. No entanto, ainda que as investigações apontem o envolvimento da Rússia em vários ataques relacionados ao período eleitoral americano (ver Anexo B, p. 136-137), as autoridades americanas acusam a Rússia oficialmente somente do caso de invasão da rede do DNC (BAEZNER; ROBIN, 2017).

O relatório do procurador especial Robert S. Mueller, que tinha como intuito investigar a possível relação entre a campanha de Trump e a Rússia na interferência das eleições nos EUA, revela de forma minuciosa como diferentes agências russas agiram no caso. Além das já relatadas invasões às redes do DNC e do DCCC, Mueller apresenta outras CyberOps que teriam sido conduzidas pelo GRU:

> As vítimas incluíam entidades estaduais e locais dos EUA, como juntas estaduais de eleições (SBOEs), secretários de estado e governos municipais, bem como indivíduos que trabalharam para essas entidades. O GRU também visou empresas privadas de tecnologia responsáveis pela fabricação e administração de software e hardware relacionados com as eleições, como software de registro eleitoral e assembleias de voto eletrônicas. O GRU continuou a visar essas vítimas durante as eleições de novembro de 2016 (MUELLER, 2019, p. 68, tradução própria).

Ainda de acordo com o relatório de Mueller, a agência russa conseguiu infectar algumas redes de computadores relacionadas ao sistema eleitoral meses antes das eleições:

> Pelo menos até o verão de 2016, os oficiais do GRU buscaram acesso a redes de computadores estaduais e locais explorando vulnerabilidades de software conhecidas em sites de entidades governamentais estaduais e locais. Os oficiais do GRU, por exemplo, visavam bancos de dados estaduais e locais de eleitores registrados usando uma técnica conhecida como "injeção de SQL", pela qual código malicioso era enviado ao site estadual ou local para executar comandos (como extrair o conteúdo do banco de dados). Em uma situação em aproximadamente junho de 2016, o GRU comprometeu a rede de computadores do Conselho de Eleições do Estado de Illinois, explorando uma vulnerabilidade no site da SBOE. O GRU então obteve acesso a um banco de dados contendo informações sobre milhões de eleitores registrados em Illinois, e extraiu dados relacionados a milhares de eleitores dos EUA antes que a atividade maliciosa fosse identificada (MUELLER, 2019, p. 68-69, traduação própria).

Embora tenha havido a invasão dessas redes, não foi comprovada nenhuma fraude nas eleições de 2016, o que pode indicar que a invasão efetuada pelo GRU tenha tido como objetivo descredibilizar e desacreditar a lisura do sistema eleitoral dos EUA perante a opinião pública do país (BAEZNER; ROBIN, 2017; MUELLER, 2019, USA, 2020).

Portanto, novamente o que se observa são CyberOps implementadas para demonstrar fragilidades e problemas em sistemas críticos e causar efeitos psicológicos sobre a população,

minando a confiança e credibilidade nas instituições do país. Tal observação é também defendida por Connel e Vogler (2017), como mostra o trecho abaixo:

> o Kremlin também usa a Internet para disseminar propaganda pró-Rússia e minar o apoio popular aos governos ou instituições de seus supostos rivais. Seus esforços nesse sentido se enquadram em duas categorias gerais: 1. Usar a espionagem cibernética para obter informações adversas sobre adversários políticos e, em seguida, vazar essas informações publicamente. 2. Usar "trolls" da internet (ou seja, indivíduos pagos) para criar blogs e perfis online falsos para inundar as seções de comentários de notícias com pontos de vista enganosos, falsos ou pró-russos (CONNEL; VOGLER, 2017, p. 23, traduação própria).

Outrossim, o principal componente das InfoOps russas foi a atividade realizada nas redes sociais e fóruns da internet, sob execução da API. Segundo Mueller (2019), as operações da API se concentraram nas plataformas Facebook, Youtube e Twitter ainda em 2014, sendo expandidas para o Tumblr e o Instagram em 2015.

No Facebook as atividades ocorriam por meio de contas criadas pelos operadores da API, chamados de “especialistas”. Mueller (2019) mostra que as contas se engajavam em uma série de discussões políticas em grupos da plataforma, tanto sobre pautas conservadoras quanto progressistas. De modo a amplificar as publicações com cunho político das contas dos operadores da API, a agência comprou mais de 3.500 anúncios que promoviam os grupos nos *feeds* da comunidade em geral (MUELLER, 2019).

Ainda no que se refere ao Facebook, estima-se que as contas controladas pelos operadores da API alcançaram dezenas de milhões de pessoas nos EUA:

> De acordo com o Facebook, no total as contas controladas pelo IRA fizeram mais de 80.000 postagens antes de sua desativação em agosto de 2017, e essas postagens atingiram pelo menos 29 milhões de pessoas nos Estados Unidos e “podem ter alcançado cerca de 126 milhões de pessoas” (MUELLER, 2019, p. 38, tradução própria).

De outro modo, no Twitter a estratégia da API foi mais complexa e envolveu tanto contas controladas por operadores da agência (*trolls*) quanto contas automatizadas (*bots*). As contas controladas pelos operadores criavam personalidades próprias para interagir com a comunidade e defendiam posições políticas fortes, de modo a atrair seguidores e aumentar o engajamento:

> A API usou muitas dessas contas para tentar influenciar o público dos EUA na eleição. [...] Usando essas contas e outras, a API provocou reações dos usuários e da mídia. Vários tweets postados pela API ganharam popularidade. Os meios de comunicação dos EUA também citaram tweets de contas controladas pela API e os atribuíram às reações de pessoas reais dos EUA. Da mesma forma, várias pessoas importantes dos EUA, incluindo o ex-embaixador Michael McFaul, Roger Stone, Sean Hannity e Michael Flynn Jr. retuitaram ou responderam a *tweets* postados nessas contas controladas pela API. Vários indivíduos afiliados à campanha de Trump também promoveram *tweets* da API [...]. (MUELLER, 2019, p. 39-40, tradução própria).

Sob outra dinâmica, as contas automatizadas ou *bots* da API, operavam para auxiliar a amplificar o alcance das pautas e temas criados pelos *trolls*:

> Em janeiro de 2018, o Twitter identificou publicamente 3.814 contas do Twitter associadas à API. De acordo com o Twitter, nas dez semanas anteriores à eleição presidencial dos Estados Unidos de 2016, essas contas postaram aproximadamente 175.993 tweets, "aproximadamente 8,4% dos quais relacionados à eleição". O Twitter também anunciou que notificou aproximadamente 1,4 milhão de pessoas que o Twitter acreditava estarem em contato com uma conta controlada pela API (MUELLER, 2019, p. 40, tradução própria).

Cabe lembrar que as postagens relacionadas aos *bots* da API sobre as eleições também foram identificadas no monitoramento da *Graphika*, conforme exposto na Figura 12. Além disso, as observações do Twitter sobre a atividades das contas automatizadas também coincidem com o período em que os EUA foram mais atacados pela campanha de desinformação russa, segundo o registro apresentado na Figura 11.

Por fim, vale ressaltar que as contas controladas pela API promoveram manifestações durante o período eleitoral nos EUA, com foco no apoio ao então candidato republicano Trump e com atos contrários à então candidata democrata Hillary Clinton. A despeito de Mueller (2019) não ter concluído sobre conluio entre a campanha de Trump e a interferência russa nas eleições, tanto o procurador quanto as demais investigações conduzidas pelo Congresso dos EUA atestam que a Rússia de fato interferiu no pleito eleitoral em favor de Trump (USA, 2019; USA, 2020).

4.4.3 Conclusões

No presente caso a Rússia apresentou uma poderosa capacidade de implementar uma guerra de informação contra os EUA e, em particular, no âmbito da eleição presidencial. Foram combinadas CyberOps e InfoOps para constantemente imprimir sobre a opinião pública estadunidense um ambiente de desinformação. A mídia tradicional foi descredibilizada, teorias da conspiração se disseminaram na sociedade civil, notícias falsas eram assimiladas como verdadeiras e o resultado foi a perda de confiança e prestígio das instituições americanas, inclusive com o abalo ao sistema da democracia liberal (BAEZNER e ROBIN, 2017).

Além disso, a administração Trump se mostrou deficiente em responder às ações russas, tanto no âmbito das operações realizadas com o intuito de desestabilizar internamente os EUA quanto na esfera internacional, dada as diversas atividades militares desempenhadas pela Rússia,

como forma de demonstração de força e projeção de *hard power* (BLACKWILL, 2019; SCHWARTZ; DIAMOND, 2020).

A preferência por negociações e relações bilaterais por parte de Trump, além de retirar os EUA de iniciativas multilaterais e enfraquecer a posição do país em alguns organismos internacionais, também gerou atritos com os demais membros da OTAN. A questão sobre o orçamento da aliança foi extremamente debatida e criticada pela administração Trump, instaurando um período de crise dentro da organização, o que é benéfico estrategicamente para a Rússia (BLACKWILL, 2019; SHAPIRO, 2019).

Contudo, não há como apenas relacionar o sucesso das ações russas com a vitória de Trump e a consequente mudanças de postura em alguns pontos da política externa dos EUA. Deve ser ressaltado que durante a administração de Trump as relações entre os EUA e a Rússia continuaram piorando e entraram nos piores momentos desde a guerra fria:

- As sanções econômicas contra a Rússia foram ampliadas em virtude da interferência nas eleições de 2016 (LAYNE, 2018);
- Suspensão do Tratado de Forças Nucleares de Alcance Intermediário (da sigla em inglês, INF) (SANGER; BROAD, 2019); e
- Desentendimentos dificultaram a renovação do New Start (DW, 2021).

No entanto, os prováveis maiores resultados da guerra de informação russa contra os EUA, que teve o ápice na eleição presidencial de 2016, foram a profunda polarização política instaurada na sociedade, o surgimento de grupos políticos radicais e a fragilização dos valores democráticos e das instituições nacionais dos EUA. Todos esses fenômenos produzem efeitos sobre a estabilidade da política interna do país e, como consequência direta, a política externa dos EUA também perde solidez (BAEZNER; ROBIN, 2017; BLACKWILL, 2019; MUELLER, 2019; USA, 2019; USA, 2020).

4.5 CONCLUSÕES PARCIAIS

Este capítulo levantou e analisou quatro casos de ações russas que envolveram o emprego de recursos cibernéticos para finalidades alinhadas com a política externa e de segurança e defesa da Rússia. A partir da observação empírica pode-se compreender que a Rússia vem evoluindo e

desenvolvendo novas capacidades no ciberespaço, desde novas armas cibernéticas até a estratégia de utilização da internet, principalmente por redes sociais, para a divulgação de propaganda russa e implementação de campanhas de desinformação contra seus inimigos.

A utilização dos recursos cibernéticos, a sua combinação e articulação com outros meios, com destaque para o militar, mostrou-se satisfatória nos episódios da Geórgia e da Ucrânia. Moscou parece ter desenvolvido a sua estratégia de guerra híbrida com aplicação de forças militares especiais e convencionais em um espaço operacional previamente atacado, comprometido e subvertido a partir do ciberespaço através das CyberOps e InfoOps.

Por outro lado, os recursos cibernéticos se revelaram mais do que novos instrumentos para auxiliarem as operações militares russas na conquista de seus objetivos em campo. Na Estônia, ataques limitados ao ciberespaço tiveram alto impacto na sociedade e no governo e serviram para a Rússia testar a viabilidade e a eficiência de ferramentas não cinéticas sem se comprometer com uma resposta contundente por parte da OTAN. Já nos EUA, a execução de CyberOps sofisticadas ao serviço de uma ampla campanha de desinformação contra o país americano possibilitou a Rússia influenciar o pleito eleitoral da maior potência do mundo e, ao mesmo tempo, enfraquecer internamente o seu maior inimigo geopolítico, sem realizar qualquer tipo de ataque cinético, cujas consequências seriam não oportunas para a Rússia.

A seguir, o Quadro 6 apresenta, com base no que foi exposto e examinado, um resumo dos elementos não cinéticos (CyberOps e InfoOps) e dos elementos cinéticos (militares) empregados pela Rússia nos casos analisados no presente capítulo. O Quadro 7 serve como legenda para o Quadro 6.

Quadro 6 – Distribuição e intensidade da utilização de instrumentos cinéticos e não-cinéticos

Casos/Elementos	CyberOps	InfoOps	Op. Militares
Estônia			
Geórgia			
Ucrânia			
EUA			

Fonte: Elaborado pelo autor com base na análise feita no Capítulo 4.

Quadro 7 – Legenda do Quadro 6

Cor	Descrição
	Empregado de forma ampla.
	Empregado de forma limitada.
	Não empregado.

Fonte:Elaborado pelo autor.

5 CONCLUSÃO

Este trabalho abordou como a Rússia emprega recursos de poder cibernético como instrumento de defesa nacional de acordo com a sua política estratégica no século XXI. De acordo com o que foi apresentado na introdução, a hipótese principal que sustenta a pesquisa é a de que a Rússia emprega determinados recursos cibernéticos de acordo com uma abordagem estratégica que busca a desestabilização interna do inimigo, a incapacidade de reação e a dissuasão, a partir de uma retórica defensiva. Também fazem parte desse arquétipo outros recursos, como o econômico, o diplomático e o militar, contudo este trabalho enfatiza a relação entre o elemento cibernético e o militar dessa estratégia. Em grau secundário, se pressupõe que a escolha para o emprego desses diferentes meios dependa diretamente do país que a Rússia pretenda atacar.

Conforme foi demonstrado, a informação desempenha um papel fundamental para compreender como a Rússia age ofensivamente no ciberespaço, sendo ela um recurso estratégico para o país. Instituir um contexto de dominância informacional é primordial para que a Rússia consiga atingir seus objetivos políticos, seja para auxiliar uma invasão armada ou para influenciar em decisões e comportamentos políticos e sociais que sejam benéficos ao país, sendo essa a sistemática estratégica do emprego de recursos de poder cibernético.

Todas as ações ofensivas da Rússia analisadas que envolveram o uso de recursos cibernéticos - seja em conjunto com elementos militares ou não – estiveram relacionadas com o contexto das relações entre os países do seu entorno estratégico e a OTAN. A percepção de ameaça advinda do alargamento das fronteiras da OTAN, da absorção pela Aliança de outros países histórica, cultural e territorialmente próximos à Rússia e a potencial desestabilização do regime russo moveram o país a realizar ações ofensivas e reativas nos episódios examinados, utilizando-se dos meios necessários e possíveis. Até mesmo a suposta interferência na eleição americana em 2016 obedece à essa lógica, uma vez que a Rússia percebe a OTAN como um instrumento de política externa dos EUA e, portanto, a desestabilização da política interna americana mostrou-se uma oportunidade de arrefecer a assertividade da política externa do país.

De acordo com o que foi analisado, a Rússia possui um robusto e descentralizado aparato institucional para agir no ciberespaço. De agências de segurança e inteligência até contatos extraoficiais com grupos organizados da sociedade civil, o país conta com muitas alternativas para

executar operações no ciberespaço, podendo inclusive fazer uso da anonimidade em alguns casos para se eximir de acusações de ingerência.

Apesar de descentralizado, o aparato russo opera de forma organizada e articulada com os demais setores da burocracia do país, inclusive com as forças armadas: nos casos da Geórgia e Ucrânia, ficou demonstrado que as operações militares foram executadas de modo coordenado com CyberOps e InfoOps. Em adição, o aperfeiçoamento constante dessas capacidades, tanto no campo das CyberOps quanto das InfoOps podem ser acompanhados pela expansão das ações russas no ciberespaço e fora dele, o que pode significar a utilização dessas técnicas para objetivos outros além dos principais previstos pela política de segurança e defesa do país: frear o avanço da OTAN e concretizar a influência russa em seu entorno estratégico.

Ademais dos resultados que possam surgir em termos de aumento do poder internacional da Rússia, as ações do país no ciberespaço devem despertar o interesse dos acadêmicos e das autoridades governamentais para as ameaças que podem advir desse tipo de abordagem. Se, por um lado, as operações militares em larga escala como as perpetuadas pela Rússia na Geórgia e na Ucrânia sejam limitadas à esfera dos países da CEI, as CyberOps e InfoOps, por outro lado, são passíveis de serem implementadas contra qualquer Estado, independentemente do poder relativo deste.

Portanto, da perspectiva teórica das Relações Internacionais, novos estudos e debates acadêmicos devem ser elaborados e pensados em torno do arcabouço teórico que discute o poder cibernético e as suas implicações no sistema internacional. O presente trabalho revelou que os encadeamentos advindos do exercício do poder no ciberespaço vão além da esfera coercitiva que se reflete em potencial ameaça às infraestruturas críticas nacionais, sendo essas entendidas no âmbito das estruturas físicas essenciais para o funcionamento da sociedade civil, dos setores público e privado nacionais.

Mais do que isso, o exercício do poder cibernético pelo Estado pode ter e, de fato tem, efeitos práticos sobre a consciência pública e por sua vez, sobre a estabilidade das instituições de Estado e de governo. Nesse contexto, outras estruturas – dessa vez as abstratas, constituídas pelos valores, dogmas e costumes - devem entrar para o rol de elementos críticos, com especial atenção para as instituições e sistemas que compõem o Estado Democrático de Direito.

Desse modo, uma série de questões devem ser levantadas e analisadas pelas autoridades nacionais responsáveis. A proteção de dados e informações dos cidadãos é um assunto complexo

que deve estar na pauta legislativa e ser debatido com o restante da sociedade, uma vez que esses são elementos que podem ser explorados por outros Estados e por pessoas e grupos mal-intencionados.

Do ponto de vista do setor tecnológico, é essencial que sejam criadas e aperfeiçoadas ferramentas capazes de identificar e coibir comportamento não humano na internet, especialmente em plataformas digitais sociais. Contudo, esse tipo de abordagem deve envolver a participação e supervisão da sociedade e ser realizado de forma transparente, para que se garanta o exercício da livre expressão no meio virtual.

Além disso, as agências de checagem de informações e notícias realizam um papel fundamental na defesa da informação embasada e confiável. Tais organizações devem receber mais apoio e visibilidade no meio digital e fora dele, de modo a conscientizar o público sobre a importância de basear opiniões e conclusões em informações checadas e confirmadas.

REFERÊNCIAS

ACÁCIO, P. D. I. Segurança Internacional no século XXI: o que as teorias de Relações Internacionais têm a dizer sobre o ciberespaço? *In*: **Relações Internacionais Cibernéticas (CiberRI): Oportunidades e Desafios para os Estudos Estratégicos e de Segurança Internacional**. Marcos Aurélio Guedes de Oliveira (Org.), Ricardo Borges Gama Neto, Gills Vilar Lopes (Org.). Coleção Defesa e Fronteiras Virtuais, v. 3. Recife: Editora UFPE. 2016. Academy of the United Kingdom. 2009. Dispónivel em: http://conflictstudies.org.uk/files/04.pdf. Acesso em 31 de julho de 2020.

ADLER, Emanuel. **O construtivismo no estudo das relações internacionais**. Lua Nova [online]. 1999, n.47, pp.201-246. ISSN 0102-6445. https://doi.org/10.1590/S0102-64451999000200011. Disponível em: https://www.scielo.br/scielo.php?script=sci_abstract&pid=S0102-64451999000200011&lng=pt&nrm=iso&tlng=pt. Vários acessos.

AJIR, M; VAILLIANT, B. Russian Information Warfare: Implications for Deterrence Theory. **Strategic Studies Quartely**, vol. 12, n° 3, 2018. Disponível em: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Ajir.pdf. Acesso em: 25 de agosto de 2020.

ARCHIVE.ORG. CNN interactive. Cold War experience. **Inside the KGB. An interview with retired KGB Maj. Gen. Oleg Kalugin**. c2020. Disponível em: http://web.archive.org/web/20070627183623/http://www3.cnn.com/SPECIALS/cold.war/episodes/21/interviews/kalugin/. Acesso em 20 de agosto de 2020.

AYRES PINTO et al. **Russia, BRICS and Cyber Power: Evoking Synergies under Conjectures of Deviation**. Journal of China and International Relations. Special Edition. Aalborg University Press. March, 2020. Disponível em: https://journals.aau.dk/index.php/jcir/article/view/4239/3669. Acesso em: 20 de março de 2020.

AYRES PINTO, J. D; MORAES, I As mídias digitais como ferramentas de manipulação de processos eleitorais democráticos: uma análise do caso Brexit. **Revista de Estudios Sociales**, vol. 74. Uniandes Journals. 2020. Disponível em: https://revistas.uniandes.edu.co/doi/abs/10.7440/res74.2020.06. Acesso em: 15 de outubro de 2020.

BAEZNER, M; ROBIN, P. Hotspot Analysis: Cyber-conflict between the United States of America and Russia. **Center for Security Studies (CSS)**. CSS Cyber Defense Project. 2017. ETH Zürich: Zurich. Disponível em: https://www.researchgate.net/publication/322364378_Cyber-conflict_between_the_United_States_of_America_and_Russia. Acesso em: 12 de janeiro de 2021.

BARNES, B. **The Nature of Power**, Cambridge: Polity. 1988.

BARTLES, K. Charles. Getting Gerasimov Right. **Military Review**. Army University Press. Jan-fev, 2016. Disponível em: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2016/. Acesso em: 12 de abril de 2020.

BARTOSH, A. A. HYBRID WAR STRATEGY AND CONSTRUCTION STRATEGY. Military Thought. **Military Theoretical Journal**. Ministry of Defense of the Russian Federation. Oct, 2018. Disponível em: https://vm.ric.mil.ru/Stati/item/138034/. Acesso em: 20 de maio de 2020.

BIZEUL, D. **Russian Business Network Study**. Nov, 2007. Disponível em: http://www.bizeul.org/files/RBN_study.pdf. Acesso em: 10 de dezembro de 2020.

BLACKWILL, D. R. **Trump's Foreign Policies Are Better Than They Seem**. Council on Foreign Relations. Council Special Report n° 84. Abr, 2019. Disponível em: https://www.cfr.org/sites/default/files/report_pdf/CSR%2084_Blackwill_Trump.pdf. Acesso em: 20 de janeiro de 2021.

BLANK, Stephen. Cyber War and Information War à la Russe. *In*: PERKOVICH, George; LEVITE, Ariel E. (ed.). **Understanding Cyber Conflict: fourteen analogies**. Washington, D.C.: Georgetown University Press, 2017. p. 81-98. Disponível em: https://carnegieendowment.org/2017/10/16/cyber-war-and-information-war-la-russe-pub-73399. Acesso em: 10 abr. 2020.

BLANDY, C. **Provocation, Deception, Entrapment: The Russo-Georgian Five Day War**. Advanced Research and Assessment Group. Defence Academy of the United Kingdom, mar. 2009. [S.L.]. Disponível em: https://www.files.ethz.ch/isn/97421/09_january_georgia_russia.pdf. Vários acessos.

BOGDANOVA, S. **SOFT POWER A LA RUSSE: MAKING SENSE OF RUSSIA'S SOFT POWER APPROACH**. University of Turku. Faculty of Humanities. University of Glasgow. School of Social and Political Sciences. Erasmus Mundus International Masters in Russian, Central and East European Studies Double Degree Programme. Master's Thesis. 2016. Disponível em: https://www.academia.edu/29498084/Soft_Power_a_la_russse_Making_Sense_of_Russia_Soft_Power_Approach?email_work_card=view-paper. Acesso em: 15 de janeiro de 2021.

BOWEN, S. Andrew. **Russian Military Intelligence: Background and Issues for Congress**. Congressional Research Service (CRS). Report – R46616, nov. 2020. Disponível em: https://fas.org/sgp/crs/intel/R46616.pdf. Acesso em: 10 mar. 2021.

BRADSHAW, Samantha; BAILEY, Hannah; HOWARD, Philip N.. **Industrialized Disinformation: 2020 global inventory of organized social media manipulation**. S.L: Oxford Internet Institute, 2020. 26 p. Disponível em: https://demtech.oii.ox.ac.uk/research/posts/industrialized-disinformation/. Acesso em: 15 mar. 2021.

BRITISH BROADCASTING CORPORATION (BBC). **Russia opposition politician Boris Nemtsov shot dead**. 2015. Disponível em: https://www.bbc.com/news/av/world-europe-31665380. Acesso em: 15 de outubro de 2020.

BRITANNICA. **The Orange Revolution and the Yushchenko presidency**. [201-?]. Disponível em: https://www.britannica.com/place/Ukraine/The-Orange-Revolution-and-the-Yushchenko-presidency. Acesso em: 05 de janeiro de 2021.

BRITANNICA. Geography & Travel. Geographic Regions. **Maghreb**, region North Africa. c2021. Disponível em: https://www.britannica.com/place/North-Africa/Ancient-North-Africa. Acesso em: 10 mar. 2021.

CARNEIRO, E. M. J. **As relações entre Defesa e Soberania no Espaço Cibernético**. Associação Brasileira de Relações Internacionais. Anais. 2017. Disponível em: https://www.encontro2017.abri.org.br/resources/anais/8/1498479573_ARQUIVO_artigo_ABRI_Joao_Carneiro.pdf. Acesso em: 10 de maio de 2020.

CASTRO, T. **Teoria das Relações Internacionais**. Fundação Alexandre de Gusmão (Funag). Ministério das Relações Exteriores – MRE. Brasília. 2012. Disponível em: http://funag.gov.br/biblioteca-nova/pdf/mostraPdf/1/40/teoria_das_relacoes_internacionais. Acesso em: 09 de maio de 2020.

CHIVVIS, S. C. **Understanding Russian "Hybrid Warfare" and What Can Be Done About It**. Testimony of Christopher S. Chivvis Before the Committee on Armed Services United States House of Representatives, mar 2017. RAND Corporation; Santa Monica. Disponível em: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf**.** Acesso em: 05 de dezembro de 2020.

CIA. Central Intelligence Agency. The World Factbook. **Estonia**. Introduction. Background. 2021. Disponível em: https://www.cia.gov/the-world-factbook/countries/estonia/. Acesso em: 03 de fevereiro de 2021.

CIA. Central Intelligence Agency. The World Factbook. **Georgia**. Geography. 2020a. Disponível em: https://www.cia.gov/the-world-factbook/countries/georgia/#geography. Acesso em: 15 de dezembro de 2020.

CIA. Central Intelligence Agency. The World Factbook. **Ukraine**. Photo Details. 2021. Disponível em: https://www.cia.gov/the-world-factbook/countries/ukraine/map. Acesso em: 15 de janeiro de 2021.

CLAESSEN, Eva. Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU. **Journal of Cyber Policy**, v. 5, n. 1, p. 140-157, fev. 2020. Disponível em: https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1728356. Acesso em: 02 de fevereiro de 2021.

CLARKE, A. R; KNAKE, K. R. **Guerra Cibernética: A próxima ameaça à segurança e o que fazer a respeito**. Brasport Livros e Multimídia Ltda. 2015. *Edição Kindle*.

CLAUSEWITZ, Carl von. **On War**. Oxford Word´s Classics. Oxford University Press Inc. Nova York. 2007.

CONNELL, M; VOGLER, S. **Russia´s Approach to Cyber Warfare**. Center for Naval Analyses. Washington, DC. Março, 2017. Disponível em: https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf. Acesso em 12 de fevereiro de 2020.

CONGRESS RESEARCH SERVICE (CRS). **Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues**. 2009. Disponível: https://www.everycrsreport.com/files/20090317_RL31787_291375f13deb5a3f48da06b5c443d1ed18686524.pdf. Acesso em: 20 de agosto de 2020.

CONFESSORE, N. **Cambridge Analytica and Facebook: The Scandal and the Fallout So Far**. The New York Times. Abril, 2018. Disponível em: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Acesso em: 10 de março de 2021.

COPADATA. Products. Zenon Software Platform. Visualization and Control with Zenon. **What is SCADA?** [s.d.]. Disponível em: https://www.copadata.com/en/product/zenon-software-platform-for-industrial-automation-energy-automation/visualization-control/what-is-scada/. Acesso em: 10 de março de 2021.

DE HAAS, M. Russia´s Foreign Security Policy in the 21st Century: Putin, Medvedev and beyond. **Contemporary Security Studies**. London and New York: Routledge. 2010.

DEUTSHE WELLE (DW). **US, Russia agree to extend 'New START' nuclear arms treaty**. Top Stories. News. 2021. Disponível em: https://www.dw.com/en/us-russia-agree-to-extend-new-start-nuclear-arms-treaty/a-56354318. Acesso em: 04 de fevereiro de 2021.

E-ESTONIA. **E-Estonia guide**. 2020b. Disponível em: https://e-estonia.com/wp-content/uploads/e-estonia-guide-210820.pdf. Acesso em: 20 de novembro de 2020.

E-ESTONIA. **E-Estonia toolkit**. 2020c. Disponível em: https://e-estonia.com/e-estonia-toolkit/. Acesso em: 20 de novembro de 2020.

E-ESTONIA. **We have built a digital society and we can show you how**. 2020a. Disponível em: https://e-estonia.com/. Acesso em: 29 de novembro de 2020.

ENISA. European Union Agency for Cybersecurity. Glossary: **Malware**. 2020. Disponível em: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/malware. Acesso em 20 de junho de 2020.

FERNANDES, José Pedro Teixeira. A ciberguerra como nova dimensão dos conflitos do século xxi. **Relações Internacionais**, Lisboa, n. 33, p. 53-69, mar. 2012. Disponível em <http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1645-91992012000100005&lng=pt&nrm=iso>. Vários acessos.

FIIA. Finnish Institute of International Affairs. **Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine**. Helsinki: Grano Oy. 2016. Disponível em: https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport45_fogoffalsehood.pdf. Acesso em: 25 de agosto de 2020.

FIREEYE. **CYBER ATTACKS ON THE UKRAINIAN GRID: WHAT YOU SHOULD KNOW**. 2016. Fireeye Industry Intelligence Report: Milpitas. Disponível em: https://www.fireeye.fr/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf. Acesso em: 12 de janeiro de 2021.

FIREYE. **APT28: At the Center of the Storm: Russia Strategically Evolves it´s Cyber Operations**. Fireeye iSight Intelligence. Special Report, jan. 2017. Disponível em: https://www.fireeye.com/current-threats/apt-groups/rpt-apt28.html. Acesso em: 18 de janeiro de 2021.

FOUCAULT, M. **Discipline & Punish: The Birth of the Prison**. Vintage editions (reprint edition), 1995.

GALEOTTI, M. **Putin´s Hydra: Inside Russia´s Intelligence Services**. European Council on Foreign Relations. 2016. Disponível em: https://www.jstor.org/stable/pdf/resrep21577.pdf?refreqid=excelsior%3A79a356b924768240251964c42cb40881. Acesso em: 18 de agosto de 2020.

GERASIMOV, Valery. Ценность науки в предвидении Новые вызовы требуют переосмыслить формы и способы ведения боевых действий. **Military Industrial Commission of the Russian Federation newspaper**. Fev, 2013. Disponível em: https://vpk-news.ru/articles/14632. Acesso em: 12 de abril de 2020.

GHERNAOUTI, S. **Cyber Power: Crimes, Conflict and Security in Cyberspace**. Forensic Sciences. EPFL Press. 2016. Disponível em: https://www.routledge.com/Cyber-Power-Crime-Conflict-and-Security-in-Cyberspace/Ghernaouti-Helie/p/book/9780429101328. Acesso em: 15 de maio de 2020.

GIL, Antonio Carlos. **Métodos e Técnicas de Pesquisa Social**. 6. ed. São Paulo: Atlas, 2008.

GILES, Keir. **"Information Troops" – a Russian Cyber Command?** 3rd International Conference on Cyber Conflict, 2011. The NATO Cooperative Cyber Defence Centre of Excellence: Tallinn. Disponível em: https://www.ccdcoe.org/uploads/2018/10/InformationTroopsARussianCyberCommand-Giles.pdf. Acesso em: 10 de dezembro de 2020.

GILES, Keir. **Handbook of Russian Information Warfare**. North Atlantic Treaty Organization (NATO) Defense College. Roma. Nov, 2016a. Disponível em: https://www.researchgate.net/profile/Keir_Giles/publication/313423985_Handbook_of_Russian_Information_Warfare/links/5899ff4eaca2721f0db11d16/Handbook-of-Russian-Information-Warfare.pdf. Acesso em: 15 de fevereiro de 2020.

GILES, Keir. Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power. **The Royal Institute of International Affairs**. Chatam House. 2016b. Disponível em: https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf. Acesso em: 25 de julho de 2020.

GOMES, P; ALVES, V. Clausewitz, a Ciberguerra e a Guerra Russo-Georgiana. **Revista Carta Internacional**, v. 15, n. 3, p. 232-254. 2020. Belo Horizonte. Disponivel em: https://www.cartainternacional.abri.org.br/Carta/article/view/1065/812. Acesso em: 08 de dezembro de 2020.

GRAPHIKA. **Secondary Infektion. Exposing Secondary Infektion**. 2020. Disponível em: https://secondaryinfektion.org/. Acesso em: 18 de outubro de 2020.

GREENBERG, A. **Sandworm: A new era of cyberwar and the hunt for the Kremlin´s most dangerous hackers**. Doubleday: New York. 2019 [pdf].

GUTTERMAN, S; BRYANSKI, G. **Putin says U.S. stoked Russian protests**. World News. Reuters. Dez, 2011. Disponível em: https://www.reuters.com/article/us-russia-idUSTRE7B610S20111208. Acesso: 19 de janeiro de 2021.

GUZZINI, S. **Max Weber´s Power em Max Weber and International Relations**. Cambridge University Press. 2017. Cambridge, RU. Disponível em: https://www.cambridge.org/core/books/max-weber-and-international-relations/EBAAF4CA76B9684E3151E65E89FCFA80. Acesso em: 15 de maio de 2020.

GUZZINI, S. **Power analysis: Encyclopedia entries**. Danish Institute for International Studies. Disponível em: www.jstor.org/stable/resrep13431. Acesso em: 20 de maio de 2020.

HAMMES, X. Thomas. **The Sling and The Stone: on War in the 21st Century**. Zenith Press. 2004.

HART, S; HESS, D. **Boris Yeltsin and the First Chechen War**. National Defense University. National War College. Course 5601 Fundamentals of Statecraft. SEMINAR I. 2001. Washington, DC. Disponível em: https://apps.dtic.mil/sti/citations/ADA441554. Acesso em: 10 de agosto de 2020.

HATCH, B. The Future of Strategic Information and Cyber-Enabled Information Operations. **Journal of Strategic Studies**, v. 12, n. 4, 2019. Disponível em: https://scholarcommons.usf.edu/jss/vol12/iss4/4/?utm_source=scholarcommons.usf.edu%2Fjss%2Fvol12%2Fiss4%2F4&utm_medium=PDF&utm_campaign=PDFCoverPages. Acesso em: 15 de setembro de 2020.

HERZOG, S. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. **Journal of Strategic Security**, vol. 4, n° 2, summer 2011: Strategic Security in the Cyber Age. 2011. Washington, DC. Disponível em: https://scholarcommons.usf.edu/jss/vol4/iss2/4/. Acesso em: 15 de novembro de 2020.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). **Key Areas of Action**. c2021. Disponível em: https://www.itu.int/en/action/Pages/default.aspx. Acesso em: 10 de março de 2021.

JAITNER, Margarita. **Russian Information Warfare: Lessons From Ukraine**. Nato Cooperative Cyber Defence Centre Of Excellence, Tallinn, p. 87-94, 2015. Disponível em: https://ccdcoe.org/uploads/2018/10/Ch10_CyberWarinPerspective_Jaitner.pdf. Vários Acessos.

JAITNER, M; MATTSSON, A. P. **Russian Information Warfare of 2014.** 7th International Conference on Cyber Conflict: Architectures in Cyberspace, 2015. The NATO Cooperative Cyber Defence Centre of Excellence: Tallinn. Disponível em: https://www.ccdcoe.org/uploads/2018/10/Art-03-Russian-Information-Warfare-of-2014.pdf. Acesso em: 10 de janeiro de 2021.

JORDAN, T. **Cyberpower: The Culture and Politics of Cyberspace and the Internet**. Routledge. Taylor & Francis Group. 1999. Londres e Nova York.

KASPERSKY. **BlackEnergy APT Attacks in Ukraine**. Resource Center. Threats. 2017. Disponível em: https://www.kaspersky.com/resource-center/threats/blackenergy. Acesso em: 11 de janeiro de 2021.

KASPERSKY. Kaspersky Lab. Resource Center. **What is Spear Phising?** 2020. Disponível em: https://www.kaspersky.com/resource-center/definitions/spear-phishing. Acesso em: 21 de junho de 2020.

KLEPPER, David. **Cyborgs, trolls and bots: A guide to online misinformation**. Associated Press (AP), fev. 2020. Disponível em: https://apnews.com/article/4086949d878336f8ea6daa4dee725d94. Acesso em: 10 de março de 2021.

KUEHL, T. D. From Cyberspace to Cyberpower: Defining the Problem. *In*: **Cyberpower and National Security**. KRAMER, D. Franklin; STARR, H. Stuart; Wentz, K. Larry (Orgs.). Potomac Books Inc.; 1st edition. 2009.

KUEHL, T. **Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age**. International Law Studies – Volume 76. Computer Network Attack and International Law. U.S. Naval War College. 2002. Disponível em: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1400&context=ils. Acesso em: 20 de agosto de 2020.

LAMAZIERE, C. **PROBLEMATIZANDO O CONCEITO DE PODER EM FOUCAULT E SUAS CONSEQÜÊNCIAS PARA PENSAR O POLÍTICO NA TEORIA DE RELAÇÕES INTERNACIONAIS**. Tese de Doutorado. Pontifícia Universidade Católica do Rio de Janeiro – PUC-RIO. Rio de Janeiro. Maio de 2009. Disponível em: https://www.maxwell.vrac.puc-rio.br/colecao.php?strSecao=resultado&nrSeq=13569@1. Acesso em: 10 de maio de 2020.

LAYNE, N. **U.S. imposes fresh Russia sanctions for election meddling**. Autos. Reuters. Dez, 2018. Disponível em: https://www.reuters.com/article/us-usa-russia-sanctions-treasury-idUSKCN1OI27F. Acesso em: 25 de janeiro de 2021.

LEWIS, James A. **THE ROLE OF OFFENSIVE CYBER OPERATIONS IN NATO'S COLLECTIVE DEFENCE**. The Tallinn Papers, Tallinn, p.1-12, jan. 2015. Disponível em: https://ccdcoe.org/library/publications/tallinn-paper-the-role-of-offensive-cyber-operations-in-natos-collective-defence/. Vários Acessos.

LIANG, Q; Xiangsui, W. **Unrestricted Warfare**. People´s Liberation Army Literature and Arts Publishing House. Pequim, China. Fev, 1999.

LILLY, B; CHERAVITCH, J. **The Past, Present, and Future of Russia's Cyber Strategy and Forces**. 2020 12th International Conference on Cyber Conflict (CyCon), Estonia, 2020, pp. 129-155. Disponível em: https://ieeexplore.ieee.org/document/9131723. Acesso em: 20 de março de 2021.

LIND et al. The Changing Face of War: Into the Fourth Generation. **Marine Corps Gazette**, oct 1989, pp. 22-26. 1989. Disponível em: https://globalguerrillas.typepad.com/lind/the-changing-face-of-war-into-the-fourth-generation.html. Acesso em: 18 de maio de 2020.

LOOKINGGLASS. **Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare**. Lookingglass Cyber Threat Intelligence Group, abr. 2015. Disponível em: https://www.lookingglasscyber.com/wp-content/uploads/2015/08/Operation_Armageddon_Final.pdf. Acesso em: 10 de janeiro de 2021.

MAKARYCHEV, Andrei. The Medvedev presidency: Russia´s changing profile. **Barcelona Centre For International Affairs.** Nizhny Novgorod, p. 165-171. [s.d.]. Disponível em: https://www.cidob.org/en/content/download/25703/313655/file/ANDREI+MAKARYCHEV_ANG.pdf. Acesso em: 10 mar. 2021.

MANKOFF, J. **Russian Foreign Policy: The return of Great Power Politics**. Maryland: Rowman & Littlefield Publishers, Inc. 2009.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de Metodologia Científica**. 5. ed. São Paulo: Atlas, 2003.

MEARSHEIMER, J. J. **The Tragedy of Great Power Politics**. W. W. Norton & Company. Updated edition. Abril, 2014.

MICROSOFT. Documentation. Previous Version. SQL. **SQL Server 2008 R2**. Security and Protection (Database Engine). Threat and Vulnerabilitty Mitigation (Database Engine). SQL Injection. 2012. Disponível em: https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2008-r2/ms161953(v=sql.105)?redirectedfrom=MSDN. Acesso em: 10 de março de 2021.

MIELNICZUK, F; PICCOLLI, L. Política e Sociedade na Rússia atual. **Em Debate**, v.7, n.4, p. 50-54. Belo Horizonte. Setembro, 2015. Disponível em: http://opiniaopublica.ufmg.br/site/files/artigo/07-Dossie-Setembro-2015-Fabiano-Mielniczuk-Larlecianne-Piccolli-Politica-e-sociedade-na-Russia-atual.pdf. Acesso em: 15 de agosto de 2020.

MORGENTHAU, J. H. **A Política entre as Nações: A luta pelo poder e pela paz**. Instituto de Pesquisa de Relações Internacionais. Editora Universidade de Brasília (UnB). Imprensa Oficial do Estado de São Paulo. São Paulo. 2003.

MOSHES, Arkady. Russia's European policy under Medvedev: how sustainable is a new compromise?. **International Affairs: Royal Institute of International Affairs**. Oxford, p. 17-30. jan. 2012. Disponível em: https://www.jstor.org/stable/41428538?seq=1#metadata_info_tab_contents. Acesso em: 10 mar. 2021.

MUELLER, S. R. **Report On The Investigation Into Russian Interference In The 2016 Presidential Election, vol. I of II**. U.S. Department of Justice. Submitted Pursuant to 28 C.F.R. § 600.8(c). Mar, 2019. Washington, DC. Disponível em: https://www.justice.gov/storage/report.pdf. Acesso em: 10 de outubro de 2020.

NATO. North Atlantic Treaty Organization. **What is NATO?** 2020. Disponível em: https://www.nato.int/nato-welcome/. Acesso em: 08 de novembro de 2020.

NETO, F. B. Walfredo. Territorializando o “novo” e (re) territorializando os tradicionais: a cibernética como espaço e recurso de poder. *In*: **Segurança e Defesa Cibernética: da fronteira física aos muros virtuais**. FILHO, M. Oscar; NETO, F. B. Walfredo; GONZALES, L. M. Selma (Orgs.). Coleção Defesa e Fronteiras Virtuais, v.1. Recife: Editora UFPE. 2014.

NEW YORK TIMES. **Cambridge Analytica and Facebook: The Scandal and the Fallout So Far**. 2018. Disponível em: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

NILSSON, N. **Russian Hybrid Tactics in Georgia**. Central Asia-Caucasus Intitute and Silk Road Studies Program, 2018. Institute for Security and Development Policy: Estocolmo-Nacka. Disponível em: https://www.researchgate.net/profile/Niklas_Nilsson2/publication/324602520_Russian_Hybrid_Tactics_in_Georgia/links/5ad86daa458515c60f589f40/Russian-Hybrid-Tactics-in-Georgia.pdf?origin=publication_detail. Acesso em: 10 de dezembro de 2020.

NYE, Joseph S. Jr.. **Cyber Power**. Harvard Kennedy School: Belfer Center for Science and International Affairs. Cambridge, p. 1-24. maio 2010. Disponível em: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a522626.pdf>. Acesso em: 21 nov. 2019.

OEC. Observatory of Economic Complexity. **Country: Russia**. 2020. Disponível em: https://oec.world/en/profile/country/rus. Acesso em: 15 de julho de 2020.

PICCOLLI, L. **Europa enquanto condicionante da Política Externa e de Segurança da Rússia: o papel da Defesa Antimíssil**. Dissertação (Mestrado em Estudos Estratégicos Internacionais) – Universidade Federal do Rio Grande do Sul, Faculdade de Ciências Econômicas, Programa de Pós-Graduação em Estudos Estratégicos Internacionais. Porto Alegre. 2012. Disponível em: https://lume.ufrgs.br/bitstream/handle/10183/70019/000875346.pdf?sequence=1&isAllowed=y. Acesso em: 30 de julho de 2020.

POLYAKOVA, Alina; BOYER, Spencer P.. **The Future of Political Warfare: Russia, The West, And the Coming Age of Global Digital Competition**. Brookings - Robert Bosh Foundation: Transatlantic Iniciative, Washington, Dc, p.1-24, mar. 2018. Disponível em: https://www.brookings.edu/research/the-future-of-political-warfare-russia-the-west-and-the-coming-age-of-global-digital-competition/. Vários Acessos.

REED, J. Donald. Beyond the War on Terror: Into the Fifth Generation of War and Conflict. **Studies in Conflict & Terrorism**, 31:8, 684-722, DOI: 10.1080/10576100802206533. Aug, 2008. Colorado, USA. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/10576100802206533. Acesso em: 18 de maio de 2020.

REZEK, Francisco. **Direito Internacional Público: curso elementar**. 16 ed. Rev. ampl. e atual. 2016. Editora Saraiva.

RITTER, Daniel P.. A spirit of Maidan? Contentious escalation in Ukraine. *In*: DELLA PORTA, Donatella (ed.). **Global Diffusion of Protest: Riding the Protest Wave in the Neoliberal Crisis**. Amsterdam: Amsterdam University Press, 2017. p. 191-214. (Protest and Social Movements). Disponível em: https://www.jstor.org/stable/j.ctt1zkjxq0.11?seq=1#metadata_info_tab_contents. Acesso em: 10 mar. 2021.

RT. **About RT**. [202-?]. Disponível em: https://www.rt.com/about-us/. Acesso em: 10 mar. 2021.

RUSNÁKOVÁ, S. Russian New Art of Hybrid Warfare in Ukraine. **Slovak Journal of Political Sciences**, v. 17, n. 3-4, p. 343-380. 2017. Disponível em: https://www.researchgate.net/publication/321955926_Russian_New_Art_of_Hybrid_Warfare_in_Ukraine/fulltext/5a3b5765aca2729d50648d0c/Russian-New-Art-of-Hybrid-Warfare-in-Ukraine.pdf?origin=publication_detail. Acesso: 10 de janeiro de 2020.

RUSSIA. Russian Federation. **Doctrine of Information Security of the Russian Federation**. Approved by Decree of the President of the Russian Federation n° 646 of December 5, 2016a. 2016a. Disponível em: https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163. Acesso em: 10 de março de 2020.

RUSSIA. Russian Federation. **Foreign Policy Concept of the Russian Federation**. Approved by President of the Russian Federation Vladimir Putin on November 30, 2016. 2016b. Disponível em: https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248. Acesso em: 10 de março de 2020.

RUSSIA. Russian Federation. **Military Doctrine of the Russian Federation**. Approved by the President of the Russian Federation Vladimir Putin. 2014. Disponível em: https://www.offiziere.ch/wp-content/uploads-001/2015/08/Russia-s-2014-Military-Doctrine.pdf. Acesso em: 10 de março de 2020.

RUSSIA. Russian Federation. **Russian National Security Strategy**, December 2015. 2015. Disponível em: http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf. Acesso em: 10 de março de 2020.

RUSSIA. Russian Federation. **The Foreign Policy Concept of the Russian Federation (2008)**. President of Russia. 2008. Disponível em: http://en.kremlin.ru/supplement/4116. Acesso em: 05 de agosto de 2020.

SANGER, E. D; BROAD, J. W. U.S. **Suspends Nuclear Arms Control Treaty With Russia. Politics**. The New York Times. Fev, 2019. Disponível em: https://www.nytimes.com/2019/02/01/us/politics/trump-inf-nuclear-treaty.html. Acesso em: 28 de janeiro de 2021.

SAWKA, R. **Putin: Russia's Choice**. New York: Routledge, 2008.

SCHMIDT, C. B. **Realism and facets of power in international relations.** Power in world politics, London, Routlegde, 2007.

SCHWARTZ, A; DIAMOND, C. **Russian Hard Power Projection: A Brief Synopsis**. Center for Strategic & International Studies. Blog Post: The Post-Soviet Post. Mar, 2020. Disponível em: https://www.csis.org/blogs/post-soviet-post/russian-hard-power-projection-brief-synopsis. Acesso em: 21 de janeiro de 2021.

SEGRILLO, A. **Os Russos**. Coleção Povos e Civilizações. Editora Contexto. 2012.

SELHORST, Tony. **Russia's Perception Warfare. The development of Gerasimov's doctrine in Estonia and Georgia and it's application in Ukraine**. Militaire Spectator. Jaargang 185 nummer 4, 2016. Disponível em: https://www.militairespectator.nl/sites/default/files/uitgaven/inhoudsopgave/Militaire%20Spectator%204-2016%20Selhorst.pdf. Acesso em: 21 de maio de 2020.

SHANE, S. **Russian Intervention in American Election Was No One-Off**. Politics. News Analysis. The New York Times. Jan, 2017. Disponível em: https://www.nytimes.com/2017/01/06/us/politics/russian-hacking-election-intelligence.html. Acesso em: 18 de janeiro de 2021.

SHAPIRO, J. **A very American crisis: Why Trump is still NATO's biggest problem**. European Council on Foreign Relations. Commentary. Dez, 2019. Disponível em: https://ecfr.eu/article/commentary_a_very_american_crisis_why_trump_is_still_natos_biggest_problem/.

SHARLET, R. Russian Constitutional Crisis: Law and Politics under Yel´tsin. **Post-Soviet Affairs**. 9:4, p. 314-336. Maio, 2013. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/1060586X.1993.10641373. Acesso em: 10 de julho de 2020.

SHVEDA, Y; HO PARK, J. Ukraine's revolution of dignity: The dynamics of Euromaidan. **Journal of Eurasian Studies**, v. 7, n. 1, p. 85-91. Jan, 2016. Disponível em: https://www.sciencedirect.com/science/article/pii/S1879366515000305. Acesso em: 06 de janeiro de 2020.

SINGER, W. P; FRIEDMAN, A. **Cybersecurity and Cyberwar: what everyone needs to know**. Oxford University Press; 1 edition. Janeiro, 2014.
SLAY, B. An interpretation of the Russian Financial Crisis. Post-Soviet and Economics. 40:3, p. 206-214. Routledge. Londres. 1999. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/10889388.1999.10641112. Acesso em: 10 de agosto de 2020.

SOLDATOV, A; BOROGAN, I. **Russia´s approach to cyber: the best defence is a good offence. Em Hacks**, Leaks and Disruptions: Russian Cyber Strategies. Institute for Security Studies. European Union. Paris: Chaillot Papers. 2018. Disponível: https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf. Acesso em: 10 de agosto de 2020.

SPUTNIK. Sputnik International. **About us**. 2021. Disponível em: https://sputniknews.com/docs/about/index.html. Acesso em: 10 mar. 2021
STONE, O. As Entrevistas de Putin: As conversas que deram origem ao documentário. 1° ed – Rio de Janeiro: Best Seller. 2017.

SVARIN, D. The construction of 'geopolitical spaces' in Russian foreign policy discourse before and after the Ukraine crisis. **Journal of Eurasian Studies**. Hanyang University. vol. 7, p. 129-140. 2016. Disponível em: https://journals.sagepub.com/doi/10.1016/j.euras.2015.11.002. Acesso em 14 de agosto de 2020.

THE GUARDIAN. **Russia accused of unleashing cyberwar to disable Estonia**. Maio, 2007. Disponível em: https://www.theguardian.com/world/2007/may/17/topstories3.russia. Acesso em: 15 de novembro de 2020.

THE STATE OIL COMPANY OF THE AZERBAIJAN REPUBLIC (SOCAR). Activities. Transportation. **Baku-Tbilisi-Ceyhan (BTC) Main Export Oil Pipeline**. 2020. Disponível em: http://www.socar.az/socar/en/activities/transportation/baku-tbilisi-ceyhan-btc-main-export-oil-pipeline. Acesso em: 12 de dezembro de 2020.

THORNTON, R; MIRON, M. Deterring Russian cyber warfare: the practical, legal and ethical constraints faced by the United Kingdom. **Journal of Cyber Policy**, v. 4, n. 2, 2019. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/23738871.2019.1640757?journalCode=rcyb20. Acesso em: 15 de outubro de 2020.

TOFT, P. John J. Mearsheimer: an offensive realist between geopolitics and power. **Journal of International Relations and Development**, v. 8, p. 381–408, 2005. doi:10.1057/palgrave.jird.1800065. Disponível em: https://link.springer.com/article/10.1057/palgrave.jird.1800065. Acesso em: 09 de maio de 2020.

TURNER, S. **Despolitizing Power. Knowledge and Power: Toward a Political Philosophy of Science by Joseph Rouse; The Nature of Power by Barry Barnes**. Sage Publications, Ltd. Social Studies of Science, vol. 19, n° 3. Aug. 1989. Disponível em: https://www.jstor.org/stable/285086?seq=1. Acesso em: 15 de maio de 2020.

UN. United Nations. UN E-Government Knowleadgebase. **Estonia**. Data Year 2020. 2020. Disponível em: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/57-Estonia/dataYear/2020. Acesso em: 05 de dezembro de 2020.

UNESCO. United Nations Educational, Scientific and Cultural Organization. Journalism. **'Fake News' and Disinformation: A Handbook for Journalism Education and Training**. c2018. Disponível em: https://en.unesco.org/fightfakenews. Acesso em: 10 mar. 2021.

USA. United States of America. Senate. **Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election: Volume 2: Russia's Use of Social Media, with Additional Views**. Out, 2019a. Disponível: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1001&context=senatedocs. Acesso em: 10 de março de 2021.

USA. United States of America. Department of Justice. Office of Public Affairs. Justice News. **Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace**. Out, 2020. Disponível em: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and. Acesso em: 15 de janeiro de 2021.

USA. United States of America. Senate. **Report of the Select Committee on Intelligence on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 5: Counterintelligence Threats and Vulnerabilities**. United States Senate. 2020. Disponível em: https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf. Acesso em: 10 de agosto de 2020.

VAN NIEKERK, Brett; MAHARAJ, Manoj. Social Media and Information Conflict**. International Journal of Communication**, v. 7, p. 1.162-1184, 2013. Disponível em: https://ijoc.org/index.php/ijoc/article/view/1658. Acesso em: 15 de janeiro de 2021.

VEN BRUUSGAARD, K. Russian Strategic Deterrence. **Survival - Global Politics and Strategy**, vol. 58, n° 4. Routledge. 2016. Disponível em: https://www.tandfonline.com/doi/full/10.1080/00396338.2016.1207945. Acesso em: 08 de agosto de 2020.

VENTRE, D. **"Ciberguerra"**. XIX Curso Internacional de Defensa. Seguridad global y potências emergentes em un mundo multipolar (Zaragoza: Imprenta Ministerio de Defensa, 2012), p. 32-45.

VENTRE, D. O dilema da fronteira virtual: quando os estados se tornam construtores de ciberfronteiras. **Dilema: Revista de Estudos de Conflito e Controle Social**, Rio de Janeiro, ed. especial n. 3, p. 75-96, 2019. Disponível em: https://revistas.ufrj.br/index.php/dilemas/article/view/23117/14951. Acesso em: 12 out. 2020.
VISITESTONIA. Estonian history and Culture. 2020. Disponível em: https://www.visitestonia.com/en/why-estonia/estonian-history-and-culture. Acesso em: 09 de novembro de 2020.

WALTZ, N. K. **Theory of International Politics**. Waveland Press; 1 edition. 2010.

WEBER, M. **Wirtschaft und Gesellschaft. Grundriss der verstehenden Soziologie**, Tübingen, 1922.

WENDT, A. (1999). **Social Theory of International Politics**. Cambridge Studies in International Relations. Cambridge: Cambridge University Press. doi:10.1017/CBO9780511612183. Disponível em: https://www.cambridge.org/core/books/social-theory-of-international-politics/0346E6FDC74FECEF6D2CDD7EFB003CF2. Acesso em: 12 de maio de 2020.

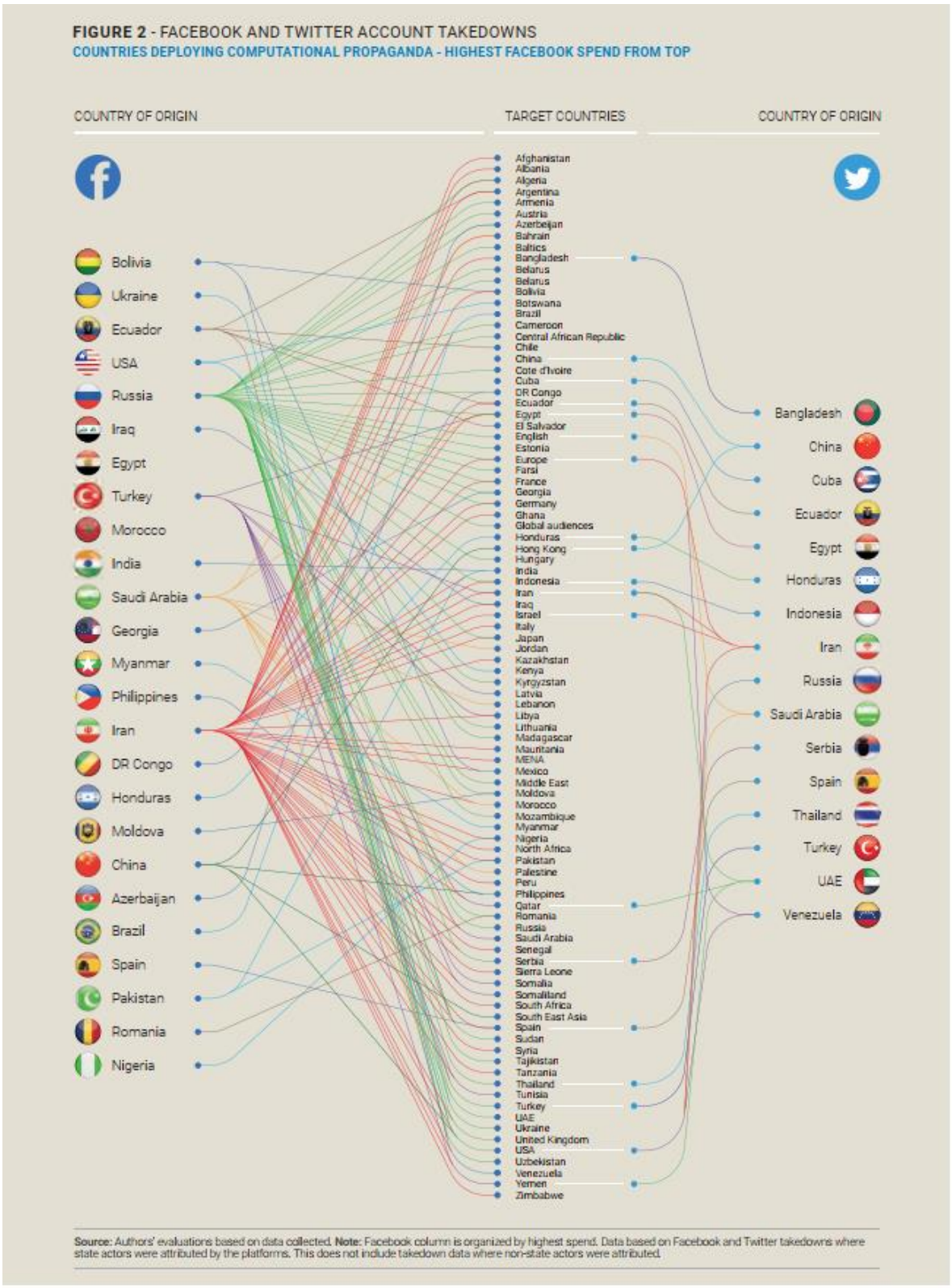
WENDT, A. A ANARQUIA É O QUE OS ESTADOS FAZEM DELA: A CONSTRUÇÃO SOCIAL DA POLÍTICA DE PODER. Tradução de Rodrigo Duque Estrada. Monções: **Revista de Relações Internacionais da UFGD**, Dourados, v.2. n.3, jan./jun., 2013. Disponível em: https://ojs.ufgd.edu.br/index.php/moncoes/article/view/2188. Vários Acessos.

WORLD BANK. **World Bank Open Data**. 2020. Disponível em: https://data.worldbank.org/. Acesso em: 05 de maio de 2020.

ZETTER, K. Hacker Lexicon: **What Is a Backdoor?** 2014. Disponível em: https://www.wired.com/2014/12/hacker-lexicon-backdoor/. Acesso em: 10 de janeiro de 2021.

ZETTER, K. **Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid: The hack on Ukraine's power grid was a first-of-its-kind attack that sets an ominous precedent for the security of power grids everywhere**. 2016. Disponível em: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. Acesso em: 10 de janeiro de 2021.

ANEXO A – CONTAS REMOVIDAS PELO FACEBOOK E TWITTER (01/2019-11/2020)



Fonte: Bradshaw, Bailey e Howard (2020).

ANEXO B – DIFERENTES TÉCNICAS USADAS NOS ATAQUES CIBERNÉTICOS

G = government institutions, M = Media, PP = Political Party, IO = International Organization				
Date	**Victim**	**Type of victim**	**Technique / Tool**	**Damage**
10.2014	US State Department unclassified network	G	Spear phishing with a malicious link	Access to thousands of computers across the USA and in embassies Access to sensitive information that could be relevant to foreign intelligence services Theft of emails concerning the Ukrainian conflict (Howarth, 2015)
10.2014	White House unclassified network	G	Spear phishing with a malicious email coming from the US State Department	Access to sensitive information available on the unclassified network, including the President's daily schedule (Perez and Prokupecz, 2015)
Early 2015	Pentagon unclassified network	G	Use of unspecified old vulnerabilities in the network	Unknown (Crawford, 2015)
Summer 2015	First breach into DNC network	PP	Spear phishing with a malicious link or attachment	Embarrassing emails later published on the Wikileaks and DCLeaks websites (Taylor, 2016)
07.2015	US Joint Chiefs of Staff email server	G	Spear phishing emails forwarded from a university previously targeted by a phishing wave	Stolen personnel credentials, passwords, and information with no intelligence value. After the network was taken down, it took the US Joint Chiefs of Staff almost two weeks to restart their email servers (Martin, 2016; Starr, 2015).

03.2016	Second breach into the DNC network and John Podesta's email account	PP	Spear phishing email disguised as one coming from Gmail	Embarrassing emails later published on the Wikileaks and DCLeaks websites and research on Republican candidate Donald Trump (Krieg and Kopan, 2016)
07.2016	Arizona and Illinois voter registration system	G	Use of unspecified malware	Theft of 20,000 personal data from voters in Illinois No data was stolen in Arizona (Lartey, 2016; Reuters, 2016)
07.2016	DCCC and Clinton's election campaign networks	PP	Spear phishing similar to the DNC case	Access to voter analysis data (McCain Nelson and Peterson, 2016)
08.2016	NSA and Equation group servers	G	Unspecified	Information, a list of IP addresses of hacked servers and a claimed malware sample later auctioned on social media (Goodin, 2016; Greenberg, 2016)
09.2016	World Anti-Doping Agency	IO	Phishing	Stolen medical files of athletes (Ingle, 2016).
12.2016	US Election agency	G	SQL Injection	Stolen list of user names and passwords, later tried to be sold on the "underground electronic markets" (Barysevich, 2016; Menn, 2016)

Fonte: Baezner e Robin (2017).