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

LUCAS MACHADO GUIMARÃES JOTA

A INFORMAÇÃO COMO ELEMENTO DE DIFUSÃO DE PODER NO ESPAÇO CIBERNÉTICO: O USO DE INTELIGÊNCIA DE FONTES ABERTAS (OSINT) NO CONFLITO ENTRE RÚSSIA E UCRÂNIA

FLORIANÓPOLIS
2022

LUCAS MACHADO GUIMARÃES JOTA

A INFORMAÇÃO COMO ELEMENTO DE DIFUSÃO DE PODER NO ESPAÇO CIBERNÉTICO: O USO DE INTELIGÊNCIA DE FONTES ABERTAS (OSINT) NO CONFLITO ENTRE RÚSSIA E UCRÂNIA

Trabalho de Conclusão de Curso apresentado ao Departamento de Economia e Relações Internacionais da Universidade Federal de Santa Catarina, como requisito parcial à obtenção do título de Bacharel em Relações Internacionais.

Orientadora: Profª Drª Graciela de Conti Pagliari

FLORIANÓPOLIS

2022

Lucas Machado Guimarães Jota

A Informação como elemento de Difusão de Poder no Espaço Cibernético: o uso de Inteligência de Fontes Abertas (OSINT) no conflito entre Rússia e Ucrânia

Florianópolis, 25 de Julho de 2022.

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

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

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

Profª. Me. Jéssica Maria Grassi
Universidade Federal de Santa Catarina

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
Graciela de Conti Pagliari
Data: 01/08/2022 07:56:28-0300
CPF: 659.263.070-15
Verifique as assinaturas em https://v.ufsc.br

_____

Profª. Drª. Graciela de Conti Pagliari
Orientadora

Florianópolis, 2022

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus pela oportunidade de poder trilhar os caminhos da vida até aqui, com saúde e com a companhia da minha família e amigos.

Agradeço aos meus pais, Hilário e Nelci, pelo suporte incondicional em todos os momentos, por investirem na minha educação desde sempre, por acreditarem no meu potencial e confiarem em minhas escolhas, por me ensinarem seus valores e princípios. Sem vocês, eu nada seria.

Agradeço à minha namorada, Pollyanne, por sempre me incentivar a seguir adiante, por me fazer acreditar em um futuro lindo, por crer que tudo daria certo, mesmo nos momentos em que minha fé esmorecia.

À minha professora e orientadora, Profª Graciela, agradeço imensamente por topar o desafio de um trabalho proposto com muita ambição e pouco prazo, pela compreensão acerca das dificuldades ao longo da pesquisa, por estar sempre disponível em cada momento dessa jornada. Por me incentivar no GESED e pela confiança na carta de recomendação do intercâmbio.

À minha estimada professora mineira Iara, pela confiança e pelas belas palavras na carta de recomendação do intercâmbio.

Aos amigos e amigas que dividiram comigo a vivência da graduação na UFSC, em especial à Jamila e à Andrezza, pelo apoio nos momentos difíceis e pela companhia nos momentos de felicidade. Aos colegas da USAC pelos inesquecíveis momentos em Floripa, em especial ao Renato pela confiança no estágio e pela oportunidade no intercâmbio. À amiga gringa Glorimar, por ser um anjinho na minha vida.

Muita coisa mudou desde 2015. A todos aqueles que fizeram parte dessa jornada, meus sinceros agradecimentos.

If information is power, why are the powerful so ill informed?

(Arthur Curley)

RESUMO

A sociedade global contemporânea vive a Era da Informação, marcada pela ultra conectividade e pela expansão da internet. Inovações nas Tecnologias de informação e Comunicação impactam um conjunto cada vez maior de aspectos da vida moderna: comunicações, serviços, economia e comércio, relações interpessoais, saúde e educação, entre outros. Nesse contexto de consolidação da cibernética, a informação ganha importância como fonte de poder no sistema internacional, e novos atores emergem ao se apropriar dessa capacidade para buscar seus interesses políticos. Um exemplo de inovação tecnológica que recentemente ganhou popularidade é a Inteligência de Fontes Abertas (OSINT), uma metodologia de coleta e análise de dados publicamente disponíveis na internet que vem sendo utilizada por indivíduos e grupos de indivíduos para monitorar diversos tipos de eventos, desde queimadas e desmatamento ilegal a violações de Direitos Humanos e conflitos militares. Este trabalho tem como objetivo investigar a informação como fonte de poder internacional, focando na dimensão cibernética e em seu uso por atores não estatais. Para tanto, busca-se, inicialmente, estabelecer uma fundamentação teórica acerca do poder nas Relações Internacionais, realçando o papel da informação. Serão apresentados os espaços onde esse poder da informação se manifesta (Ambiente Informacional, Espaço Cibernético e Internet), bem como os conceitos de Poder Cibernético e Poder Informacional, presentes na literatura sobre o tema. Também serão apresentadas as principais características da OSINT, dentro do método de produção de conhecimento denominado Atividade de Inteligência, e ressaltados os aspectos nos quais essa metodologia converge com a Revolução Digital e com a atuação de atores não estatais. Em um segundo momento, propõe-se um estudo de caso referente ao conflito armado em andamento entre Rússia e Ucrânia, notadamente marcado pela dimensão cibernética e informacional. O objetivo será analisar o monitoramento, via Fontes Abertas, da mobilização e da concentração de recursos militares russos nas proximidades da fronteira com a Ucrânia, em contraposição às declarações oficiais do Kremlin. Espera-se que seja possível exemplificar de que maneiras o acesso à informação permite a atores não-estatais exercer poder, em especial no que tange ao soft power e às três dimensões relacionais (coerção, controle sobre a agenda e estabelecimento de preferências). Empenhar-se-á, também, em ilustrar a tendência de aumento da relevância do poder informacional e a redistribuição deste tipo de poder no sistema internacional. Constata-se que a essa revolução informacional e digital resulta em um aumento da importância do poder informacional no arsenal de capacidades disponíveis aos diversos atores, seja por propiciar

vantagens em termos de recursos de poder, seja pela sua relevância no que tange ao Soft Power e à construção de narrativas que legitimem as ações estatais. Particularmente, o estudo de caso apresentado possibilita explanar a agência de atores não estatais em relação ao controle de agenda, efetivamente limitando a capacidade do governo russo de influenciar a opinião pública internacional acerca dos eventos na Ucrânia.

Palavras-chave: Espaço Cibernético; Informação; OSINT; Poder Informacional; Rússia; Ucrânia.

ABSTRACT

Contemporary global society lives the Information Age, distinguished by an ultra connectivity and by the expansion of the internet. Innovations in Information and Communication Technologies impact an increasing number of aspects of modern life: communications, services, economy and commerce, interpersonal relationships, health and education, among others. In this context of consolidation of cybernetics, information enhances its significance as a source of power in the international system, and new actors emerge while acquiring this capacity to pursue their political interests. An example of a technological innovation that recently became popular is Open Source Intelligence (OSINT), a methodology for collecting and analyzing publicly available data on the internet, that has been used by individuals and groups of individuals to monitor various types of events, from wildfires and illegal deforestation to human rights violations and military conflicts. This paper aims to investigate information as a source of international power, focusing on the cybernetic dimension and its use by non-state actors. To achieve this goal, we initially seek to establish a theoretical foundation about power in International Relations, highlighting the role of information. The spaces where the power of information manifests (Informational Environment, Cyberspace and the Internet) will be presented, as well as the concepts of Cyber Power and Informational Power, present in the literature on the subject. The main characteristics of OSINT will also be presented, within the method of knowledge production called Intelligence Activity, underscoring the aspects in which this methodology converges with the Digital Revolution and with the agency of non-state actors. In a second moment, a case study is proposed, regarding the ongoing armed conflict between Russia and Ukraine, notably marked by the cybernetic and informational dimension. The objective will be to analyze the monitoring, via Open Sources, of the mobilization and concentration of Russian military resources near the border with Ukraine, as opposed to official statements by the Kremlin. Expectedly it will be possible to exemplify how access to information allows non-state actors to exercise power, especially with regard to Soft Power and the three relational dimensions (coercion, control over the agenda and establishment of preferences). It will also endeavor to illustrate the trend of increasing relevance of informational power and the redistribution of this type of power in the international system. It appears that this informational and digital revolution results in an increase in the importance of informational power in the arsenal of capabilities available to the various actors, either by providing advantages in terms of power

resources, or by its relevance concerning Soft Power and the construction of narratives that legitimize state actions. In particular, the case study presented makes it possible to illustrate the agency of non-state actors in relation to agenda control, effectively limiting the Russian government's ability to influence international public opinion about events in Ukraine.

Keywords: Cyberspace; Information; OSINT; Informational Power; Russia; Ukraine.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AI Ambiente Informacional

ARPANET Advanced Research Projects Agency Network

BBC British Broadcasting Corporation

CIR Centre for Information Resilience

CyberOps Operações Cibernéticas

DDoS Distributed Deny of Service

DIME/PIME Político-Diplomático, Informacional, Militar e Econômico

DOD United States Department of Defense

EUA Estados Unidos da América

FBIS Foreign Broadcast Intelligence Service

HUMINT Human Sources Intelligence

ICANN Internet Corporation for Assigned Names and Numbers

IMINT Imagery Intelligence

InfOps Operações Informacionais

ISP Internet Service Providers

LN Liga das Nações

OCR Optical Character Recognition

OSINT Inteligência de Fontes Abertas

OTAN Organização do Tratado do Atântico Norte

PsyOps Operações Psicológicas

SAR Synthetic-Aperture Rada

SIGINT Signals Intelligence

TCP/IP Transmission Control Protocol / Internet Protocol

TIC Tecnologias da Informação e Comunicação

UE União Europeia

USRR Union of Soviet Socialist Republics

SUMÁRIO

1 INTRODUÇÃO

As transformações sociais em andamento desde o final da Guerra Fria trouxeram diversos novos fenômenos para a vida das pessoas e para a atenção de tomadores de decisão e pesquisadores. Apenas para compor o argumento, pode-se mencionar a aceleração da globalização nos anos 1990, a guerra ao terror nos anos 2000, e o recrudescimento dos nacionalismos extremos nos anos 10 do século presente. Paralelamente a esses e outros eventos, e permeando a todos, o advento da microeletrônica e das redes de computadores (dentre elas a hoje ubíqua internet) fez surgir inovações nas relações sociais, econômicas e culturais, tornando tais tecnologias objeto de interesse natural em diferentes áreas do conhecimento.

Essa revolução digital[1] fez sentir os seus impactos também nas relações internacionais. À medida que sistemas eletrônicos interconectados se expandem, se tornam essenciais a um conjunto cada vez maior de aspectos da sociedade moderna: comunicações, serviços, economia e comércio, relações interpessoais, saúde e educação. A consolidação desse mundo cibernético traz consigo um novo ambiente de interação e de projeção de poder entre os atores internacionais, dotado de peculiaridades que o distinguem das dimensões estratégicas tradicionais. Estados, organizações e indivíduos, então, buscam seus interesses e avaliam suas capacidades nesse novo domínio.

Nesse contexto, o papel de atores não estatais se torna cada vez mais proeminente, seja em tempos de paz ou de guerra. De fato, será visto adiante que características próprias do ambiente cibernético, como o anonimato e o baixo custo de entrada, têm o efeito de reduzir as assimetrias entre as capacidades dos atores, o que favorece o exercício do poder por parte desses agentes considerados menores.

Especificamente, nota-se que os atores supracitados dispõem de novas possibilidades de acesso e uso da informação. A popularização de tecnologias móveis, imagens de satélite, geolocalização e mídias sociais gera uma imensurável quantidade de dados, muitas vezes publicizados em tempo real. Além disso, muitas dessas informações podem ser consideradas sensíveis em um contexto de conflito deflagrado, seja na disputa de narrativas em busca de legitimar certas ações, seja na atribuição de responsabilidade de certos incidentes, ou mesmo

[1] Castells (1996, p. 69-76) lista cinco características da revolução tecnológica-informacional: 1) a informação é a matéria prima, e as tecnologias agem sobre ela; 2) a disseminação dos efeitos dessas novas tecnologias, devido à informação estar presente em toda atividade humana; 3) a lógica em rede dos sistemas e relacionamentos que utilizam tais tecnologias, o que favorece uma maior complexidade; 4) a flexibilidade de processos e de instituições, permitindo que se adaptem a rápidas mudanças sociais; 5) a convergência de tecnologias de alta especialização (eletrônica, biológica, física) em um sistema informacional integrado, de modo que seus avanços se tornam interdependentes.

no monitoramento de capacidades e de mobilização de recursos militares. Ao se constatar a verdade da popular frase “conhecimento é poder”, cabe então o argumento de que alguns aspectos do poder no cenário internacional estão se tornando mais acessíveis a um crescente grupo de atores.

Nesse contexto, o presente trabalho tem por objetivo geral investigar a informação como fonte de poder internacional utilizada por atores não estatais, analisando o papel da Inteligência de Fontes Abertas (OSINT[2]) a partir de um caso específico de conflito interestatal. Em vista disso, os objetivos específicos são os seguintes: (i) apresentar uma revisão teórica acerca da importância da informação para o poder nas Relações Internacionais, (ii) apresentar os espaços de exercício do poder da informação, com foco na dimensão cibernética, (iii) identificar a crescente disponibilidade de informações sensíveis ou estratégicas para atores não estatais, por meio de ferramentas como a OSINT, e (iv) investigar o caso específico do conflito entre Rússia e Ucrânia, em 2022, buscando elementos que exemplifiquem os aspectos teóricos.

De modo preliminar, Fontes Abertas são dados disponíveis publicamente, sem nenhuma restrição de acesso, como fotos e vídeos publicados em redes sociais na internet, e imagens de satélite fornecidas por plataformas gratuitas ou comerciais. Na conjuntura de uma Revolução Digital e de uma sociedade global ultra conectada, esse material público passa a incluir informações que podem ser consideradas sensíveis ou estratégicas para o Estado, como a localização de seus recursos militares no teatro de operações. Indivíduos e grupos de indivíduos, então, se apropriam de tais informações, a despeito do interesse dos atores estatais.

Dessa forma, se propõe responder ao seguinte problema de pesquisa: “Como a crescente disponibilidade de fontes abertas potencializa a ação de atores não-estatais em conflitos internacionais?”. Este trabalho se sustenta na hipótese de que "A difusão de poder, acelerada pela emergência do ciberespaço e por ferramentas como a OSINT, potencializa a ação de atores não-estatais em contextos de conflitos entre Estados”.

Para responder a essa pergunta e testar a hipótese proposta, este trabalho se divide em dois capítulos.

O primeiro, eminentemente teórico, versará sobre o conceito de poder nas relações internacionais, com foco em seu aspecto informacional. Será investigada a importância do poder da informação na literatura, culminando na descrição dos conceitos teóricos de poder informacional e poder cibernético. A apresentação do Ambiente Informacional, do Ciberespaço e da Internet é feita nesse capítulo, visando delimitar os espaços onde o poder da informação é

[2] Acrônimo do inglês Open Source Intelligence.

exercido de forma mais manifesta. Analisar-se-á, também, a relação existente entre a emergência do espaço cibernético e a agência de atores não-estatais no palco mundial, consequência da Revolução Digital e de características intrínsecas a esse domínio operacional. Posteriormente, será apresentado o método de produção de conhecimento denominado "Inteligência de Fontes Abertas", caracterizando-o como potencial recurso de poder para indivíduos e grupos de indivíduos.

O segundo capítulo consistirá em um estudo de caso referente ao conflito armado entre Rússia e Ucrânia. Esse caso concreto específico foi escolhido por ser notadamente marcado pela dimensão cibernética e informacional, e por permitir avaliar os impactos mais recentes desse novo contexto internacional.

O estudo será feito por meio da análise de fontes oficiais do governo russo, bem como da verificação de fatos realizada por grupos não governamentais que utilizaram Fontes Abertas. O objetivo é exemplificar como o acesso à informação permite que atores não-estatais exerçam poder, em especial no que tange ao *soft power* e às três dimensões relacionais (coerção, controle sobre a agenda e estabelecimento de preferências). Busca-se, também, ilustrar a tendência de aumento da relevância do poder informacional e a redistribuição deste tipo de poder no sistema, consequências de novas tecnologias e metodologias que facilitam o acesso a informações consideradas sensíveis ou estratégicas.

Considerando a delimitação supramencionada, este trabalho implementará a metodologia de estudos de casos e a abordagem hipotético-dedutiva.

Segundo Yin e Campbell (2018), o estudo de caso se torna uma boa estratégia de pesquisa quando se colocam as questões "como" e "porquê" acerca de eventos contemporâneos, sendo que o pesquisador possui pouco controle sobre os eventos e sobre o contexto. Dessa forma, essa metodologia caracteriza-se por ser um estudo detalhado e exaustivo de poucos, ou mesmo de um único objeto, fornecendo conhecimentos profundos. Essa escolha metodológica, portanto, justifica um escopo bem delimitado do caso estudado, para que se possa atingir o detalhamento necessário à análise do evento real. Nesse sentido,

> O estudo de caso é um método empírico que investiga um fenômeno contemporâneo (o "caso") em profundidade e dentro de seu contexto do mundo real, especialmente quando os limites entre o fenômeno e o contexto podem não ser claramente evidentes. Em outras palavras, você gostaria de fazer um estudo de caso porque deseja entender um caso do mundo real e assumir que tal compreensão provavelmente envolverá importantes condições contextuais pertinentes ao seu caso (YIN; CAMPBELL, 2018, p.45, tradução nossa).

Adicionalmente, de acordo com Marconi e Lakatos (2003), o método hipotético-dedutivo “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” (MARCONI; LAKATOS, 2003, p.106). Nesse sentido, serão investigados os aspectos da maior disponibilidade de informações sensíveis e do uso desse tipo de dado como fonte de poder relacional.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo tem por objetivo identificar os principais aspectos da discussão teórica sobre o poder informacional e o poder cibernético nas relações internacionais. O intuito é estabelecer as bases que orientarão o estudo de caso apresentado no capítulo subsequente. Para tanto, esta fundamentação teórica foi dividida em quatro tópicos.

Inicialmente, percorrendo os autores fundamentais da escola realista, espera-se demonstrar que não é recente o interesse da literatura por essa dimensão do poder. Será visto, também, como a análise pode ser expandida ao incorporar elementos de outras áreas do conhecimento, como Ciência Política e Sociologia. O segundo tópico busca definir os espaços onde o poder da informação se manifesta, pelo que serão apresentados os conceitos de Ambiente Informacional, de Espaço Cibernético e da própria Internet. Delimitar tais espaços e identificar suas respectivas características permitirá uma melhor compreensão quanto ao impacto da Revolução das TICs na política internacional.

Em seguida, o terceiro tópico apresenta os conceitos de Poder Informacional e Poder Cibernético, e as aproximações e divergências entre eles. Esse tópico traz, também, conceitos de uma outra área do conhecimento: a Ciência da Informação. O objetivo é compreender como a informação é fonte de poder no século XXI, e identificar estratégias de conversão de poder utilizadas nesse contexto.

Por último, o quarto tópico deste capítulo apresenta a Atividade de Inteligência, com foco nas especificidades da OSINT e na atuação de atores não estatais. Será colocado o argumento de que a combinação entre Fontes Abertas e Revolução Digital aumentou de forma expressiva o acesso de indivíduos e grupos de indivíduos a informações sensíveis ou estratégicas.

2. 1 O poder nas relações internacionais: recursos e comportamentos

O poder é um objeto de estudo central no campo de conhecimento das Relações Internacionais[3]. A discussão teórica sobre as relações de poder entre os Estados, e também entre estes e os demais atores internacionais, acompanhou as transformações políticas ao longo da história, com o objetivo de melhor explicar a conjuntura de cada época e mesmo de identificar tendências futuras ou mudanças de paradigmas.

No presente tópico, buscou-se resgatar o debate teórico acerca do poder no campo de estudo das relações internacionais. Mantendo o aspecto da informação como fio condutor ao longo dos diversos autores e correntes teóricas, será possível perceber que o tema foi considerado relevante em diferentes contextos históricos. Mesmo naquele que é considerado o tratado militar mais antigo, Sun Tzu já destacava a importância da informação no contexto de conflitos e relações de poder[4] Finalmente, pretende-se argumentar que o poder derivado da informação é parte integrante da distribuição de capacidades entre os atores internacionais, e que alterações nesta distribuição têm impacto significativo na política internacional.

Carr (1981), escrevendo no contexto dos anos 30 e da iminência da segunda guerra mundial, retoma as discussões sobre a primazia do poder na política internacional após um período de predominância da corrente liberal e de iniciativas como a Liga das Nações (LN). O autor aponta que, após a Primeira Guerra, o liberalismo passou a dominar a política internacional, e os defensores dessa corrente acreditavam que instituições como a recém estabelecida LN significariam a eliminação da força na resolução de conflitos interestatais. Porém, segundo o autor, a política de poder continuava presente, estando apenas escondida pelo monopólio do poder por parte das grandes potências aliadas, que agiam para manter o *status quo*.

Ao discorrer sobre o poder nas relações internacionais, Carr (1981) o divide em três categorias analíticas ou instrumentos, que são interdependentes entre si: Militar (Estratégico), Econômico, e Poder sobre a Opinião (Propaganda).

O Poder Militar seria de suprema importância, visto a guerra ser a *ultima ratio* do poder entre os Estados. O autor afirma que "todo ato do Estado, no aspecto do poder, está dirigido

[3] Ávila e Pinheiro (2014, p.25) afirmam que "O Estado tem como instrumento básico de sua ação o elemento poder, tanto em seus relacionamentos externos, isto é, com seus pares [demais Estados] e com os agentes supranacionais [organizações internacionais], quanto no seu relacionamento com seus próprios cidadãos. Desta forma, entender como o Estado opera, pressupõe entender como ele se articula em termos de poder."

[4] O general chinês cunhou a famosa frase "Se você conhece o inimigo e a si mesmo, não precisa temer o resultado de cem batalhas."

para a guerra, não como uma arma desejável, mas como uma arma que pode ser necessária como último recurso" (CARR, 1981, p.143), e destaca que a própria classificação dos países em "potências" considera primordialmente suas capacidades militares. O Poder Econômico, por sua vez, é salientado no contexto da mobilização total das economias para a sustentação de um conflito armado, de tal forma que a capacidade econômica de uma nação seria o equivalente ao seu potencial de guerra.

O terceiro instrumento é a Propaganda, uma forma de poder que, segundo Carr (1981), se tornou mais importante nos conflitos modernos. Isso seria consequência de uma expansão nas bases da política, o que significaria um número maior de pessoas cuja opinião é politicamente relevante:

> "Era uma condição para o sucesso nas frentes militar e econômica que o 'moral' próprio fosse mantido e que o moral do outro lado fosse solapado e destruído. A propaganda foi o instrumento pelo qual se buscou ambos esses fins." (CARR, 1981, p.176).

O posicionamento político das massas passa, então, a ser determinante para a consolidação do poder dos governantes, sejam democráticos ou totalitários, e assim os instrumentos para moldar a opinião pública ganham importância. Com a popularização da política internacional e o esmaecimento da distinção entre civis e combatentes, o Poder sobre a Opinião se consolidou como um recurso disponível no arsenal dos Estados.

Hans Morgenthau (1985), outro autor fundamental na teorização do poder na política internacional, publicou sua obra entre o final da Segunda Guerra e o que viria a se tornar a Guerra Fria. Criticando duramente a corrente liberal, o autor defende que o objetivo imediato da política é sempre a luta pelo poder, e que as demais esferas das relações humanas (econômica, legal, moral) devem ser analisadas de modo subordinado à esfera política. O poder significa o domínio de um indivíduo sobre as mentes e atitudes dos demais, e, conforme colocado pelo autor:

> O poder político consiste em uma relação entre os que o exercitam e aqueles sobre os quais ele é exercido. Ele faculta aos primeiros o controle sobre certas ações dos últimos, mediante o impacto que os primeiros exercem sobre as mentes deles. O referido impacto pode derivar de **três fontes: a expectativa de benefícios, o receio de desvantagens, e o respeito ou amor por indivíduos ou instituições.** Ele pode ser exercitado por meio de ordens, ameaças, pela autoridade ou carisma de um homem ou de um órgão, bem como pela combinação de quaisquer desses meios. (MORGENTHAU, 1985, p.51, grifo nosso)

O autor apresenta uma distinção entre o poder legítimo (respeito ou amor) e o poder ilegítimo. Trata-se de uma diferença qualitativa, que diz respeito basicamente à aceitação, por

parte do ator subordinado, daquela relação de poder. Para o autor, “o poder legítimo, que pode sempre invocar uma justificação moral ou legal para o seu exercício, tende normalmente a ser mais efetivo do que o equivalente poder ilegítimo” (MORGENTHAU, 1985, p.54). Seja devido a ideologias políticas, a conceitos universais como a autodefesa, ou ao carisma e prestígio de grandes líderes nacionais, não se pode menosprezar a importância da legitimidade que os subordinados atribuem àqueles que detêm o poder.

Percebe-se que essa fonte de poder citada por Morgenthau está, em certa medida, relacionada com o poder sobre a opinião pública elaborado por Carr. Em ambos os casos, o poder do Estado depende, ao menos em parte, da forma como o exercício deste poder é vista pelos subordinados e por terceiros. O grau de apoio da população à política externa de seu governo, a moral nacional, “proporciona um fator intangível, sem cujo apoio nenhum governo, democrático ou autocrático, seria capaz de implementar as suas políticas com plena efetividade” (MORGENTHAU, 1985, p.263). Faz sentido, então, imaginar que esta dimensão do poder seja explorada em um cenário de conflito, com cada ator buscando maximizar a sua moral e sua legitimidade, ao mesmo tempo, afetar negativamente a moral dos demais. Percebe-se que tais aspectos do poder já consideram a imagem do Estado perante seus pares e suas populações, e será visto posteriormente que a disseminação de informação e a construção de narrativas podem ser utilizadas para moldar essa imagem, positiva ou negativamente.

Carr e Morgenthau, considerados realistas clássicos, abordam o poder como um recurso ou instrumento obtido pelos Estados, um fim em si mesmo. Um ator poderoso seria aquele que possui mais recursos militares e/ou econômicos que os demais. Mesmo o aspecto informacional é tratado como um recurso de poder. A unidade que detém a melhor narrativa, o modo de vida mais atraente, a ideologia mais convincente, seria considerada mais poderosa que as outras.

Tais recursos ou instrumentos do poder nacional são frequentemente citados na literatura sobre o tema, e se manifestam de acordo com o modelo DIME/PIME: Político/Diplomático, Econômico, Informacional e Militar. Um exemplo é a definição fornecida pelo Departamento de Defesa estadunidense, que coloca os instrumentos de poder como “todos os meios disponíveis pelo governo em sua busca pelos objetivos nacionais” (DOD, 2007, p.266, tradução nossa). Nota-se que esse entendimento da informação como recurso de poder está mais relacionado ao Estado Nacional, no contexto do chamado *Hard Power*.

O cientista político estadunidense Kenneth Waltz (1986), em obra publicada em meados da década de 80, trouxe para o debate novas perspectivas a respeito dos condicionantes do poder internacional. Segundo Waltz (1986, p.47), as teorias da política internacional podem ser divididas em duas categorias: Teorias reducionistas e Teorias sistêmicas.

As abordagens reducionistas buscam explicar os resultados da política internacional em função de elementos internos aos Estados, e de suas variadas combinações. Esses elementos internos dos países são os seus recursos; por exemplo, as capacidades econômicas, sociais, militares; e seu comportamento, seja belicoso, revolucionário ou pacifista. Dados os atributos dos Estados (em especial daqueles mais importantes, as potências), no nível nacional e subnacional, seria possível determinar a realidade de todo o sistema internacional. Nas palavras do autor:

> Nações mudam em forma e propósito, avanços tecnológicos são feitos, armamentos são transformados radicalmente, alianças são forjadas e rompidas. Essas são mudanças dentro dos sistemas, e tais mudanças ajudam a explicar variações nos resultados da política internacional. (Waltz, 1986, p.55, tradução nossa).

No entanto, a variedade de resultados observados na política internacional é bem menor do que as variações identificadas na constituição das unidades. Isso significa que haveriam fatores externos às unidades, ditos estruturais, que seriam marcados por uma maior resistência à mudança.

Waltz, assim, defende a abordagem sistêmica (ou estruturalista), que reconhece a influência do sistema como um todo no comportamento de seus participantes. A estrutura internacional, nessa linha de pensamento, "emerge a partir da interação entre os Estados, e então os constrange de tomar certas atitudes, ao passo que os propele em direção a outras" (WALTZ, 1990, p.29, tradução nossa). Haveria, portanto, uma relação bidirecional entre a estrutura e suas partes, e os resultados observados na política internacional teriam suas causas originadas tanto no nível das unidades quanto no nível sistêmico.

A estrutura internacional de Waltz (1990, p.29) é caracterizada pela anarquia e pela distribuição de poder entre as unidades. O primeiro atributo fica evidenciado com a ausência de uma autoridade supranacional global. Já o segundo atributo diz respeito ao poder como um meio para se obter segurança, de modo que os Estados incorrem em riscos ao possuir poder demais ou de menos:

> "Em uma teoria estruturalista, os Estados são organizados pelo seu poder, e diferenças nessa organização ajudam a explicar tanto os seus comportamentos quanto os seus destinos. Em qualquer sistema político, a distribuição das capacidades das unidades é uma chave para a explicação." (WALTZ, 1990, p.31, tradução nossa).

Esses atributos do sistema internacional seriam úteis para explicar a continuidade de certos resultados, como a persistência de conflitos e guerras e do caráter anárquico da política internacional, ainda que tenha havido mudanças significativas no nível das unidades. Tais

fatores estruturais “agem como uma força que constrange e ordena, e por fazê-lo é que teorias sistêmicas explicam e predizem a continuidade interna de um sistema” (Waltz, 1986, p.57, tradução nossa).

A *contrario sensu*, certas mudanças no sistema internacional poderão ser melhor explicadas no nível da estrutura, quando suas causas puderem ser identificadas na variação do caráter anárquico do sistema ou, mais provavelmente, na variação da distribuição de poder. Quando ocorre, a mudança estrutural “dá origem a novas expectativas a respeito dos resultados que serão produzidos pelos atos e interações das unidades, cuja organização no sistema varia com as mudanças na estrutura” (Waltz, 1986, p.58, tradução nossa).

Em resumo, se ocorrem alterações na distribuição de poder entre as unidades, temos uma mudança essencialmente estrutural, que pode melhor esclarecer os novos resultados políticos. O presente trabalho irá arrazoar, mais à frente, que essa lógica pode levar à identificação de uma mudança estrutural no sistema internacional contemporâneo, no que tange à distribuição hodierna do poder da informação.

Em uma argumentação que se encaixa na categoria das teorias sistêmicas, Nye (2011) afirma que o poder, para além da mera posse de recursos, sempre dependerá do contexto no qual é exercido. O poder de um ator é difícil de mensurar objetivamente, pois não há uma unidade de medida que o quantifique de forma isolada. Avaliar a capacidade de um agente apenas em termos do tamanho de suas forças armadas ou de sua economia seria insuficiente para entender o porquê de a vontade de certos atores prevalecer em certas situações de disputa. Ao afirmar que “o poder depende das relações humanas, que variam em diferentes contextos”, Nye (2011, p.5, tradução nossa) constata que as relações de poder no século XXI são muito diferentes daquelas em momentos anteriores.

Assim, além de analisar o poder no que tange aos seus recursos, deve-se buscar compreendê-lo também em sua dimensão comportamental-relacional. Nye (2004) distingue, nesse sentido, duas categorias diferentes de poder: *Hard Power* e *Soft Power.* O chamado Poder Duro diz respeito à habilidade de coagir, de obter o resultado desejável por meio de incentivos ou ameaças tangíveis, e está relacionado mormente ao poderio econômico e militar de um ator.

Em oposição a este poder coercitivo, Nye (2004) identifica o Poder Brando como a capacidade de alterar comportamentos por meio da atração e da modelagem de preferências, sem que nenhuma ameaça ou troca se explicite de forma tangível na relação. Nas palavras do autor:

> O poder de comando — a capacidade de mudar o que os outros fazem — pode se basear na coerção ou na indução. O poder de cooptação – a capacidade de

> moldar o que os outros querem – pode se basear na atratividade da cultura e dos valores ou na capacidade de manipular a agenda de escolhas políticas de uma maneira que faz com que os outros deixem de expressar algumas preferências porque parecem ser demasiado irreais. Os tipos de comportamento entre comando e cooptação variam ao longo de um espectro que vai da coerção à indução econômica, à definição de agenda e à pura atração. Os recursos de poder brando tendem a ser associados à extremidade cooptativa do espectro de comportamento, enquanto os recursos de poder rígido geralmente estão associados ao comportamento de comando. (Nye, 2004, p.23, tradução nossa)

Mais do que recursos de poder, portanto, a diferenciação entre *Hard* e *Soft Power* captura o modo como o poder é exercido em uma relação. Isso é importante pois o objetivo maior dos agentes é obter os resultados que desejam em cada relação de poder, de modo que são relevantes as maneiras de se transformar recursos em resultados efetivos. Trata-se das "estratégias de conversão de poder", isto é, as habilidades de utilizar efetivamente os recursos para alterar o comportamento alheio e, assim, obter os resultados preferíveis. Para Nye (2011), essas estratégias de conversão estão intimamente relacionadas à capacidade de se combinar efetivamente os poderes Duro e Brando. A essa combinação efetiva o autor denomina *Smart Power*:

> O Smart Power vai ao cerne do problema da conversão de poder. […] os primeiros passos para o smart power e estratégias eficazes de conversão de poder são entender toda a gama de recursos de poder e reconhecer as dificuldades em combiná-los efetivamente em vários contextos (Nye, 2011, p.23, tradução nossa).

Ao se discutir a aplicação prática do poder nas relações internacionais, é necessário considerar tanto os recursos dos atores quanto o contexto no qual eles interagem, e ainda quais são as estratégias de conversão utilizadas.

Dessa forma, Nye (2011, p.10-18) expande o quadro de análise ao evidenciar o caráter relacional do poder e as diferentes estratégias para sua efetivação. Para melhor elaborar as diferentes formas com as quais o poder se manifesta nas relações, o autor recorre a definições clássicas da área da ciência política. Citando autores que balizam o debate nessa área, Nye (2011) sistematiza os diferentes comportamentos de poder, classificando-os em três faces ou dimensões: Comando da mudança, controle de agenda, e estabelecimento de preferências.

Nye (2011) cita a primeira face do poder conforme definida pelo cientista político Robert Dahl. Essa dimensão do poder diz respeito à habilidade de fazer o outro agir de forma contrária às suas preferências iniciais. É uma dimensão coercitiva do poder, e o ator que a exerce pode ser considerado mais poderoso à medida que são mais fortes as preferências iniciais do ator que a sofre, e em relação ao quanto essas preferências são alteradas no decorrer da relação.

Os poderes militar e econômico são exercidos primariamente nesta face coercitiva, embora também seja possível identificar seus efeitos nas demais dimensões. Nota-se, assim, que essa dimensão está intimamente relacionada com as capacidades de *Hard Power*.

Citando os cientistas políticos Peter Bachrach e Morton Baratz, Nye (2011) destaca a segunda face do poder, que trata da definição ou enquadramento da agenda. Por agenda, entende-se o conjunto de temas que os atores envolvidos aceitam debater, bem como a lista de possíveis ações, relacionadas a esses temas, que tais atores admitem como legítimas ou viáveis. Essa dimensão se diferencia da primeira pois não possui um caráter coercitivo, mas sim de cooptação ou aliciamento. Nas palavras de Nye, "o enquadramento de agenda foca na habilidade de manter certas questões fora da mesa de negociação" (Nye, 2011, p.12, tradução nossa). O que importa é o reconhecimento da legitimidade da agenda por parte do polo passivo da relação de poder. Se, por outro lado, a agenda é controlada por meios coercitivos, então este controle é, na verdade, a aplicação da primeira face do poder. Por utilizar mecanismos como persuasão e atração, essa dimensão do poder faz parte do que Nye chama de *Soft Power*.

A terceira face do poder envolve a capacidade de definir as preferências iniciais dos demais atores. Nye (2011) evidencia esse terceiro aspecto conforme a definição do sociólogo Steven Lukes. Nesse caso, ao invés de modificar o comportamento das unidades no polo passivo, o Estabelecimento de Preferências significa que o ator no polo ativo da relação consegue fazer com que o seu resultado preferencial seja adotado pelos demais atores desde o princípio. Não seria, então, necessária nenhuma estratégia de coerção ou de persuasão, diferenciando essa terceira dimensão daquelas exercidas pelo comando da mudança ou pelo enquadramento da agenda. Vale reforçar que essa terceira face do poder também está intimamente relacionada com o *Soft Power*, de acordo com Nye:

> O poder de comando (a primeira face) é muito visível e facilmente compreendido. É a base para o poder duro – a capacidade de obter os resultados desejados por meio de coerção e pagamento. O poder de cooptação das faces dois e três é mais sutil e, portanto, menos visível. Ele contribui para o soft power, a capacidade de obter resultados preferidos através dos meios cooptativos de definição de agenda, persuasão e atração. (Nye, 2011, p.16, tradução nossa)

Essa decomposição do comportamento de poder em três dimensões será relevante para que se identifique como o poder derivado da informação se manifesta em cada tipo de relação de poder. Nesse sentido, cabe o argumento de que a informação pode ser utilizada para coação, para restrição de agenda ou mesmo para a definição de interesses iniciais do oponente. Uma vez que a disseminação das Tecnologias de Informação e Comunicação amplia o papel da informação em todos os aspectos da sociedade, percebe-se como a dimensão cibernética pode

significar, em cada uma das faces, novas formas de comportamento de poder e novos atores com capacidade para perpetrá-lo.

Em outras palavras, como atores não estatais carecem, via de regra, de poder coercitivo, o entendimento do poder em suas três faces relacionais possibilita identificar as outras maneiras pelas quais esses atores podem obter seus resultados desejados. Além disso, a segunda e a terceira faces do poder constituem o que Nye (2011, p.14) chama de "aspecto estrutural do poder", isto é, elementos da relação que não dependem diretamente da decisão particular dos atores, e sim do contexto sistêmico no qual estão inseridos. Isso reflete o caráter estrutural do *soft power* e, por conseguinte, reforçará o argumento da mudança estrutural causada pela disseminação do poder derivado da informação.

Tabela 1 - As três faces do poder relacional

	Primeira Face	**Segunda Face**	**Terceira Face**
	Induzir outros a fazer o que, de outra forma, não fariam	Enquadramento de Agenda	Moldar as preferências iniciais do outro
Hard:	A usa força/pagamento para mudar as estratégias existentes de B	A usa força/pagamento para truncar a agenda de B (quer B goste ou não)	A usa força/pagamento para moldar as preferências de B ("síndrome de Estocolmo")
Soft:	A usa atração/persuasão para mudar as preferências existentes de B	A usa atração ou instituições para que B veja a agenda como legítima	A usa atração e/ou instituições para moldar as preferências iniciais de B

Fonte: elaboração própria, com base em Nye (2011, p.91)

Com essa definição sistêmica do poder em mente, Nye (2004, p.20) aponta que a distribuição de poder no mundo moderno poderia ser visualizada como um complexo tabuleiro tridimensional de xadrez

O tabuleiro superior é fortemente dominado pelo poder militar, de caráter predominantemente coercitivo. Trata-se de uma dimensão que abrange as questões interestatais clássicas como território e disputas fronteiriças. Neste aspecto da política internacional, faz sentido apontar a unipolaridade dos EUA como única superpotência militar global. Destarte, nota-se que o xadrez nesse primeiro tabuleiro é jogado em termos de *Hard Power* e da primeira face do poder relacional.

Já no tabuleiro intermediário, a multipolaridade do poder econômico se faz presente, sendo este também intimamente ligado à primeira face do poder e a capacidades coercitivas. Nye (2004, p.20) cita apenas as relações econômicas entre Estados nesse segundo aspecto,

embora também se possa questionar sobre o papel exercido por organizações internacionais e de grandes empresas multinacionais.

Finalmente, o palco internacional inferior é caracterizado pela a-polaridade das relações transnacionais, pela presença de diversos atores não-estatais, e por uma maior difusão de poder entre os atores. É neste tabuleiro inferior que a revolução informacional gera as maiores mudanças, e que o *Soft Power* se apresenta como uma forma de poder mais eficaz em atingir os resultados desejáveis. O Estado mantém o seu monopólio nas discussões dentro dos dois primeiros tabuleiros, porém se vê obrigado a dividir o palco com novos tipos de atores no terceiro. Nesse novo contexto, "as redes e a conectividade se tornam uma fonte importante de poder" (NYE, 2011, p.xvii, tradução nossa).

Nye (2004, p.20) busca esclarecer, então, que o jogo da política mundial se desenvolve nos três tabuleiros acima, concomitantemente. A depender do assunto envolvido e do resultado esperado, os atores devem articular suas capacidades tanto verticalmente quanto horizontalmente, combinando *hard* e *soft power* ao longo das dimensões militar, econômica e transnacional.

Por uma outra linha de pensamento, retomando a lógica de Waltz (1986), é possível argumentar que esse terceiro tabuleiro, referente às relações transnacionais, vem se tornando uma fonte de mudança estrutural na política internacional. Como visto anteriormente, a estrutura da política internacional é definida pelo seu caráter anárquico e pela distribuição de poder entre as unidades. Esses aspectos estruturais, em regra, sofrem pouca variação, e mesmo as mudanças que podem ser identificadas ao longo da história ocorrem, em regra, de forma gradual.

Entretanto, ao expandir o conceito de poder para incluir suas dimensões não coercitivas, torna-se perceptível uma redistribuição de certos aspectos do poder entre os variados atores do sistema. Ainda que o caráter anárquico permaneça, e que a distribuição de capacidades coercitivas resista a variações súbitas e substanciais[5], a disseminação das TICs e a difusão do *Soft Power* alteram a estrutura de maneira que os agentes, estatais ou não, têm de lidar com novos constrangimentos em suas interações.

Logo, considerando que este terceiro tabuleiro é marcado pela proliferação de atores não-estatais, visualiza-se uma relação entre o poder da informação e o aumento de capacidade de indivíduos e grupos.

---

[5] Não se ignora aqui as recentes mudanças regionais na distribuição de poder coercitivo, como a ascensão da China e da Rússia. Apenas buscou-se manter como referência todo o sistema internacional.

Este primeiro tópico buscou percorrer a discussão teórica acerca do poder nas relações internacionais, evidenciando a importância da informação como fonte de poder para Estados e atores não-estatais. A princípio, o entendimento da informação como um instrumento do poder nacional corrobora a relevância desse aspecto na política internacional, embora acabe por restringir essa capacidade ao Estado.

Por outro lado, a ampliação do conceito de poder, de modo a incluir estratégias não-coercitivas para a obtenção dos resultados desejados, é essencial para que a análise capture a atuação de indivíduos e grupos nessas relações. Ademais, no nível da estrutura, o próprio fato de que certas capacidades estão disponíveis a novos atores significa uma mudança de contexto, isto é, uma mudança na distribuição de poder, que gera novos constrangimentos e limita as ações possíveis no sistema.

No tópico seguinte, serão elaborados com mais detalhes os diferentes espaços nos quais o poder da informação se manifesta. A revolução da informação e a consolidação da cibernética serão analisadas, de modo a entender como esses fatores puderam alterar rápida e significativamente a distribuição de poder, em especial o poder da informação, no sistema internacional.

2. 2 Ambiente informacional, ciberespaço e internet

Os três termos acima muitas vezes se confundem e, em alguns contextos, são usados como sinônimos. No entanto, é importante defini-los e diferenciá-los, para que se possa entender melhor essa esfera onde os atores interagem e projetam poder, e as mudanças geradas pela evolução tecnológica.

Neste tópico, será abordada a relação entre os conceitos de Ambiente Informacional, Ciberespaço e Internet, bem como será investigado o impacto da revolução digital na configuração destes ambientes. Espera-se elucidar de que modo a informação é usada como fonte de poder no Ambiente Informacional, e como esse aspecto do poder tem ganhado relevância no contexto do século XXI. Sobretudo, busca-se demonstrar que o poder informacional está se tornando cada vez mais acessível a indivíduos e grupos, que passam a utilizar essa nova capacidade no palco da política internacional.

2. 2. 1 O Ambiente Informacional

Iniciando pelo conceito mais amplo, o Ambiente Informacional (AI) pode ser definido como "o agregado de indivíduos, organizações e sistemas que coletam, processam, disseminam ou agem sobre a informação" (DOD, 2014, p.I-1 ix, tradução nossa). O AI precede, portanto, o desenvolvimento de tecnologias de informação e comunicação, visto que esse ambiente engloba todas as formas de informação possíveis, sejam analógicas ou digitais, sejam manipuladas por meios cibernéticos ou tradicionais.

Percebe-se, ainda, que o conceito de AI adotado neste trabalho engloba tanto os aspectos da tecnologia utilizada (*hardware* e *software*) como também o aspecto humano, ou seja, os variados atores que utilizam a informação para fins diversos. A definição estabelecida pelo Departamento de Defesa estadunidense classifica tais aspectos em três dimensões sinérgicas que compõem o AI: Física, Informacional e Cognitiva:

> A dimensão física é composta pelos sistemas de comando e controle, tomadores-chave de decisão, e a infraestrutura de suporte que habilita indivíduos e organizações a criarem efeitos. A dimensão informacional especifica onde e como a informação é coletada, processada, armazenada, disseminada e protegida. A dimensão cognitiva engloba as mentes daqueles que transmitem, recebem e respondem à ou agem sobre a informação. (DOD, 2014, p.I-1 x, tradução nossa)

Kuehl (2009, p.7) denomina essas três dimensões como Conectividade, Conteúdo e Cognição, respectivamente. As dimensões do conteúdo e da cognição podem ser consideradas

"tradicionais", no sentido de que ambas sofreram poucas alterações devido à Revolução Digital. Segundo Alberts et al. (2001, p.10-14), a esfera informacional está mais relacionada com a informação em si, que foi capturada do mundo real por algum observador, e passa a estar disponível para armazenamento e tratamento. Embora se possa argumentar que a Era Digital aumentou a quantidade de informação disponível e facilitou o seu compartilhamento, a informação por si só continua sendo, como antes, uma entidade capturada do mundo físico e posteriormente compreendida pela cognição humana.

De forma similar, a esfera cognitiva manteve a sua característica definidora: o aspecto humano do ambiente informacional. Ainda que hodiernamente a sociedade esteja imersa na revolução digital, os participantes continuam a obter informações sobre o mundo real, seja diretamente ou por intermédio da dimensão informacional, e sempre tais informações são compreendidas através de suas percepções, crenças, ideologias e valores particulares. A forma de criação e obtenção de informações mudou, o volume e o acesso às informações são incomparáveis, mas a interação entre os três domínios do AI permanece. Em outras palavras,

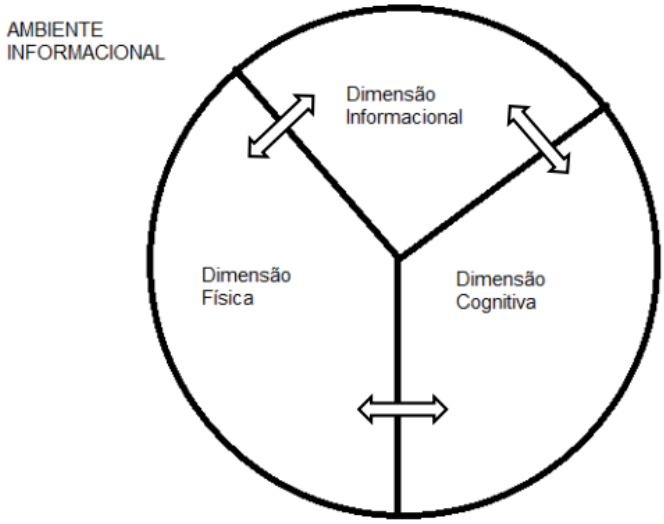
> "Há apenas uma realidade, ou domínio físico. Esta é convertida em dados selecionados, informação e conhecimento, pelos sistemas no domínio informacional. Por meio de treinamentos e da experiência compartilhada, tentamos fazer com que as atividades cognitivas de tomadores de decisão militares se tornem similares, todavia elas permanecem únicas a cada indivíduo, [..]" (ALBERTS et al., 2001, p.13, tradução nossa)

O domínio físico, por sua vez, pode ser entendido como o mundo real, onde objetos e eventos ocorrem. Tal realidade pode ser capturada de forma direta pelos sentidos humanos, sendo então transformada em um simulacro e representada na esfera cognitiva. Ela pode ser, ainda, mapeada indiretamente por meio da tecnologia, de modo a ser inicialmente representada na esfera informacional, para posteriormente ser assimilada pela percepção humana.

Pode-se entender esta esfera física como a interface entre o Ambiente Informacional e os cinco domínios operacionais, pois é nela que o AI se manifesta de forma tangível para as unidades participantes. Mormente, a esfera física "é o domínio onde residem as plataformas físicas e as redes de comunicação que os as conectam" (ALBERTS et al., 2001, p.12, tradução nossa), de modo que este é o aspecto do Ambiente Informacional que teve suas características fundamentalmente alteradas pela Revolução Digital e pela Cibernética.

Percebe-se, então, que "a dimensão física/interconectada é o meio primário pelo qual o ciberespaço toca e molda o ambiente informacional, pois os aspectos tecnológicos de um mundo interconectado são dominados pelo espaço cibernético" (KUEHL, 2009, p.7, tradução nossa).

Figura 1 - Dimensões do Ambiente Informacional.



Fonte: elaboração própria, com base em ALBERTS et al. (2001)

Em outros termos, o ciberespaço consiste em apenas uma parte do Ambiente Informacional, embora seja uma parte cada vez maior e mais relevante deste. Adicionalmente, o espaço cibernético influencia todas as três dimensões do AI, seja direta ou indiretamente, visto que são dimensões interdependentes de um mesmo ambiente onde os participantes captam, armazenam e interpretam as informações. Finalmente, constata-se que o AI já existia nas relações sociais mesmo antes de se pensar em um domínio cibernético, conquanto a Revolução das TICs tenha alterado de forma significativa este ambiente.

2. 2. 2 O Espaço Cibernético

Viu-se então que o espaço cibernético, ou ciberespaço, está contido neste amplo ambiente informacional. Esse espaço operacional começa a se consolidar com o desenvolvimento de novas Tecnologias de Informação e Comunicação, em especial os dispositivos eletrônicos, que permitem à humanidade atuar em um meio físico antes inacessível: o espectro eletromagnético. Mais formalmente, de acordo com Kuehl (2009),

> Ciberespaço é um domínio global dentro do ambiente informacional, cujo caráter distintivo 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, p.4, tradução nossa)

Esse espaço é apresentado, então, como um quinto domínio onde humanidade pode operar. Os dois primeiros domínios operacionais, terra e água, são explorados pelo homem desde a antiguidade, enquanto só recentemente tornou-se possível acessar e operar nos ambientes aéreo e espacial. Cada um desses domínios possui características físicas únicas, que os diferenciam entre si. Ademais, foram necessárias inovações e tecnologias específicas para que se pudesse operar em cada um desses ambientes, e projetar poder dentro deles e entre eles.

Nota-se que a separação dos possíveis ambientes de atuação militar em cinco domínios ou dimensões operacionais é amplamente utilizada na literatura sobre o tema. Segundo Carafano (2017, p.23, tradução nossa), "A guerra é uma competição entre adversários, […] e essa competição se desenrola nos domínios acessíveis a cada competidor: terra, mar, ar, espaço e ciberespaço". Esses domínios não são conjuntos disjuntos de um mesmo universo, mas possuem interseções e influências uns sobre os outros. Em uma situação real de guerra, não é mais possível imaginar a atuação isolada em um desses domínios, pelo que as forças armadas modernas adotam conceitos como "operações conjuntas" e "forças-tarefa", onde militares das diferentes forças atuam em grupos altamente coordenados. Resumidamente,

> Os vários ambientes (terra, mar e ar) tornaram-se conhecidos como "domínios" na terminologia militar. Dentro desses domínios, as capacidades militares são aplicadas para observar, mover, defender e atacar; a maneira pela qual os objetivos militares são perseguidos varia com o ambiente em que a atividade ocorre. Os domínios são onde a atividade ocorre para criar efeitos e, finalmente, obrigar um adversário a cumprir a vontade do Estado vitorioso. (MCGUFFIN; MITCHELL, 2014, p.397, tradução nossa)

Versando ainda sobre o conceito proposto por Kuehl (2009), pode-se destacar a dicotomia entre o meio físico no qual ocorrem as atividades cibernéticas e o propósito com o qual esse espaço foi organizado e expandido.

Temos então que, por um lado, "o argumento de que o ciberespaço é um ambiente feito pelo homem é apenas meia-verdade" (KUEHL, 2009, p.5), visto que suas características físicas se baseiam em fenômenos naturais, cuja utilização exige tecnologias próprias, tal qual ocorre com os demais domínios. Da mesma forma que inovações na navegação marítima e na aeronáutica possibilitaram que mar e ar fossem utilizados para projeção de poder, a Revolução das TICs fez com que o meio eletromagnético se tornasse estratégico para os atores internacionais, sendo passível de processos de securitização e se colocando como local de exercício da política mundial.

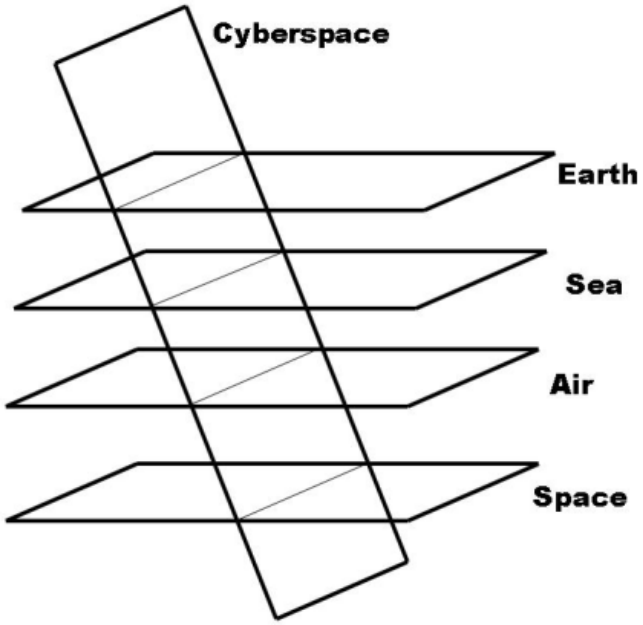
Por outro lado, "o ciberespaço é também um ambiente desenhado, criado com a intenção específica de facilitar o uso e a exploração da informação" (KUEHL, 2009, p.4). A conectividade em rede e a predominância do aspecto informacional não são características

intrínsecas ao meio físico eletromagnético, mas sim resultado de um direcionamento arbitrário no processo de desenvolvimento das tecnologias envolvidas. É essa característica que trouxe o ciberespaço para o centro dos debates nas relações internacionais. "É o acoplamento inseparável entre tecnologia, usuários humanos e o impacto da interconectividade no mundo moderno que diferencia as redes de informação atuais das anteriores." (KUEHL, 2009, p.6).

Ventre (2011) chama a atenção para a transversalidade do ciberespaço, que está intimamente ligada à essa relação do quinto domínio com o ambiente informacional:

> "Nós podemos representar o ciberespaço como um espaço transversal em relação às dimensões convencionais, colocando de lado aqui a transversalidade e globalidade do espaço [sideral], colocando-o no mesmo escalão dos demais, de modo que estaremos focados apenas na característica do espaço cibernético. **O único espaço que é verdadeiramente transversal a todos os demais é o espaço informacional, do qual o ciberespaço é um componente**." (VENTRE, 2011, p.162, tradução nossa, grifo nosso)

Figura 2 - Transversalidade do Ciberespaço



Fonte: (Ventre, 2011)

Dessa forma, a consolidação do espaço cibernético como um domínio estratégico-operacional amplia ainda mais a sobreposição entre as demais dimensões, tendo em vista a importância que a informação exerce em todas elas. Ademais, essa consolidação é consequência direta da Revolução Digital, cujo principal atributo é a expansão das TICs por todos os aspectos da sociedade moderna, seguindo uma lógica de conectividade em rede. Não se trata, portanto, de ignorar que a informação sempre foi um recurso importante para que a humanidade atuasse

em terra, mar, ar e espaço, mas sim de perceber que as peculiaridades de uma sociedade ultra conectada amplificam o papel exercido por este recurso.

É importante mencionar que muitos autores não diferenciam explicitamente o espaço cibernético do ambiente informacional. Singer e Friedman (2014, p.13) declaram categoricamente que "o ciberespaço é sobretudo um ambiente informacional" (SINGER; FRIEDMAN, 2014, p.13), embora também diferenciem o aspecto físico e humano deste ambiente. Nas palavras dos autores, "o ciberespaço é definido tanto pelo reino cognitivo quanto pelo reino físico ou digital. As percepções importam, [...]" (SINGER; FRIEDMAN, 2014, p.14). Por sua vez, Clarke e Knake (2015, p.87) parecem não dar muita atenção ao elemento humano do ciberespaço, focando mais nas diferenças entre este conceito e o da internet. Os autores escrevem que "o ciberespaço inclui a Internet, além de várias outras redes de computadores que não deveriam ser acessíveis a ela" (CLARKE; KNAKE, 2015, p.87), e procedem a discorrer sobre o funcionamento e as vulnerabilidades da rede mundial e de redes menores por ela interconectadas.

O próprio Nye (2012, p.162), muito referenciado nas discussões sobre difusão de poder, não se preocupa em elaborar uma definição própria do que seja o espaço cibernético, se limitando a citar Kuehl (2009), com adaptações. Quando muito, o autor disseca esse espaço em duas camadas: A camada física, hardware, mais vinculada ao espaço geográfico e, portanto, mais facilmente sujeita à soberania estatal; e a camada virtual, software, de difícil controle jurisdicional.

Entretanto, pode-se argumentar que a distinção entre Ambiente Informacional e Ciberespaço é essencial para uma análise cujo foco principal seja o poder derivado da informação, tal como no presente trabalho. Esse poder já estava presente na política internacional antes de surgirem a eletrônica e a cibernética, de modo que a distinção supramencionada ajuda a perceber como a revolução das TICs, ao longo de sua expansão, modificou o AI e o próprio aspecto informacional do poder. Mais especificamente, essa separação ajuda a compreender como o papel da informação na política moderna tem aumentado, uma vez que esse ganho de importância ocorre *pari passu* com a disseminação da cibernética.

Há de se destacar, ainda, duas características que são mais facilmente percebidas no ciberespaço do que nos demais domínios operacionais: a sua natureza reticular e o seu alcance global[6].

[6] Novamente, citando VENTRE (2011), o alcance global do espaço exterior é preterido para que se possa enfatizar a onipresença do aspecto informacional em todos os cinco domínios.

Primeiramente, deve-se frisar que a Revolução das Tecnologias de Informação ocorreu segundo uma lógica de expansão em rede, em contraste com a lógica hierarquizada que caracterizava as instituições anteriores. Tal lógica está na essência da expansão do ciberespaço e, conforme será visto adiante, de sua rede mais relevante, a internet. Voltando na literatura tão longe quanto o início dos anos 90, já se pode encontrar uma preocupação com o rearranjo de instituições e organizações propiciado pelas TICs. Conforme elaborado por Arquilla e Ronfeldt,

> A revolução da informação, tanto em seus aspectos tecnológicos quanto não tecnológicos, põe em movimento forças que desafiam o formato de muitas instituições. Ela rompe e corrói as hierarquias em torno das quais as instituições são normalmente projetadas. Ele **difunde e redistribui o poder, muitas vezes em benefício do que podem ser considerados atores menores e mais fracos**. […] Enquanto isso, as próprias mudanças que incomodam as instituições – a erosão da hierarquia, etc. – favorecem o surgimento de redes multi-organizacionais. De fato, **a revolução da informação está fortalecendo a importância de todas as formas de redes** – redes sociais, redes de comunicação, etc. (ARQUILLA; RONFELDT, p.26-27, tradução nossa, grifo nosso)

Esse caráter reticular favorece, portanto, a agência de atores internacionais antes marginalizados da política de poder, como indivíduos e organizações não-estatais.

Nye (2011, p.132) categoriza os atores no domínio cibernético em três amplas categorias: Governos; Redes Altamente Estruturadas, como organizações transnacionais e grupos terroristas; e Redes Fracamente Estruturadas, que são indivíduos cooperando em certas situações e para objetivos específicos. Embora os Estados ainda mantenham a maior parte dos recursos, principalmente no que concerne a capacidades coercitivas (leia-se, *hard power* e aspectos militar e econômico do poder), o contexto moderno é marcado pela presença de uma miríade de atores menores com capacidades que não podem mais ser ignoradas. Principalmente devido ao baixo custo de entrada, à anonimidade e à facilidade de saída, "[...] atores individuais no domínio cibernético se beneficiam da vulnerabilidade assimétrica em comparação com governos e grandes organizações" (NYE, 2011, p.138, tradução nossa).

Não obstante seja improvável que indivíduos atuando na internet conseguirão, por si só, subjugar governos e grandes corporações, "eles podem, com um investimento minúsculo, impor sérios custos relativos a interrupções de operações e a reputações" (NYE, 2011, p.139, tradução nossa). Nota-se, assim, uma das formas que o ciberespaço facilita o exercício de poder por parte de indivíduos e grupos.

> **Redes** [que são **um tipo importante de poder estrutural** no século 21] estão se tornando cada vez mais importantes na era da informação, e o posicionamento nas redes sociais pode ser um importante recurso de poder. […] Outro aspecto das redes que é relevante para o poder é sua extensão. **Mesmo laços extensivos fracos podem ser úteis na aquisição e**

> **disseminação de informações novas e inovadoras** (NYE, 2011, p.17, tradução nossa, grifo nosso)

A segunda característica de destaque é o alcance global do espaço cibernético. Esse alcance se consolida devido ao baixo custo na produção de dispositivos eletrônicos, permitindo que mesmo pessoas de baixo poder aquisitivo acessem às redes e o meio eletromagnético. Além de pessoas, dispositivos automatizados também se utilizam das redes para comunicarem entre si e com seus administradores, por vezes se tornando acessíveis a usuários não-autorizados e mal-intencionados. O domínio militar se beneficiou da automação e da interconexão de seus sistemas, aumentando a eficácia do comando e controle, e o domínio econômico foi favorecido pelo surgimento de novos mercados internacionais e pelos ganhos de escala propiciados pelas TICs.

Mas o alcance global do ciberespaço também está relacionado, como foi colocado acima, ao seu desenho intencionalmente focado na informação, pois esta é um componente importante de qualquer interação social. A digitalização da informação e a conexão em rede dos mais variados aspectos da vida em sociedade, desde relacionamentos pessoais a serviços empresariais e aplicações militares, tornou mais rápida, barata e acessível a informação. Por conseguinte, o domínio cibernético adquiriu uma relevância cada vez maior no Ambiente Informacional, e também fez com que o AI se tornasse mais importante em cada um dos demais domínios operacionais.

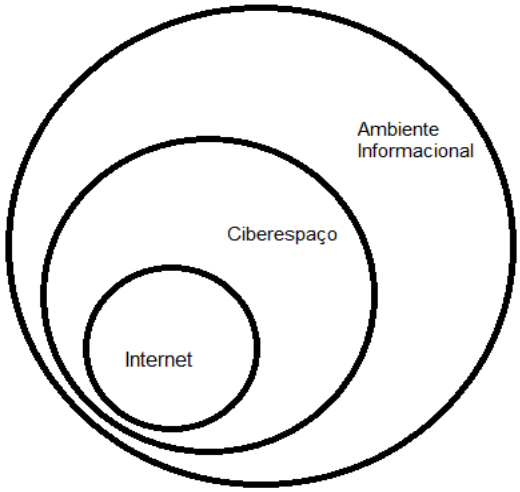
Sendo assim, a chave para compreender a importância do espaço cibernético nas relações internacionais está na conjunção entre sua arquitetura em rede, seu foco informacional e a sua quase ubiquidade em todas as interações sociais modernas. Observa-se que o meio físico eletromagnético, por si só, não possui evidente valor estratégico. As ondas de rádio e os fluxos de elétrons, isoladamente, não constituem uma ameaça à soberania dos Estados, nem mesmo influenciam as relações de poder entre os atores. É quando esse espectro é utilizado para gerar, transmitir e manipular informações, e quando esse espaço toma a forma de redes de alcance global, interconectadas e interdependentes, que a relevância do ciberespaço como domínio de projeção de poder se manifesta.

2. 2. 3 A Internet

Finalmente, a internet pode ser vista como um subconjunto do ciberespaço, constituindo-se de uma das muitas redes de dispositivos que o compõem, embora sem dúvida seja a maior delas. Esta rede global de computadores teve início como um projeto de pesquisa

acadêmica, financiado pelos militares estadunidenses nos anos 60, ainda dentro do contexto da guerra fria. A chamada ARPANET buscou interconectar redes pré-existentes de universidades, por meio de um conjunto padronizado de regras de transmissão de dados: o *Internet Protocol Suit* (Conjunto de Protocolos TCP/IP)[7].

Figura 3 - Relação entre internet, ciberespaço e ambiente informacional.



Fonte: elaboração própria

Conforme apontam Singer e Friedman (2014), "o que faz a internet única em relação a redes de comunicação anteriores […] é que ela é comutada por pacotes, ao invés de ser comutada por circuitos". Isto é, os dados transmitidos são fracionados em unidades de tamanho bem menor, chamados "pacotes", que podem seguir caminhos distintos ao longo da rede, até que atinjam o dispositivo de destino. Enquanto, na comutação por circuitos, a ligação entre dois dispositivos é direta e ocupa por completo o meio físico de transmissão entre eles, a comutação por pacotes permitiu que se compartilhasse, entre vários dispositivos, os escassos recursos de transmissão da época (cabos de cobre, fibras óticas e conexões por satélite, por exemplo).

Ademais, a comutação por pacotes permite que a internet obtenha os benefícios de uma arquitetura em rede, descentralizada. Por exemplo, se uma parte da rede fica inoperante, os pacotes de dados podem seguir uma rota alternativa para alcançar o seu destinatário final, mantendo o restante dos dispositivos em comunicação.

Outra vantagem é que adicionar um novo dispositivo à internet possui atualmente um custo marginal muito baixo, pois a infraestrutura necessária já está próxima[8]. Ainda mais

[7] Destaca-se que diversas outras redes de dispositivos modernas, como redes internas e privadas, utilizam o mesmo conjunto de protocolos, ainda que possam funcionar desconectadas da internet.
[8] Pode-se apontar alguns desafios à continuidade da expansão da internet, como por exemplo o acesso em regiões rurais e remotas. Geralmente esse desafio está mais ligado à viabilidade econômica do que à indisponibilidade de tecnologia.

interessante, a rede mundial facilita com que vários indivíduos cooperem e compartilhem informações de forma tempestiva e com cada vez mais qualidade, impulsionando a capacidade destes atores de atingirem os seus objetivos.

O aumento da importância das redes, conforme citado por Arquilla e Ronfeldt (1993) e reforçado por Nye (2011), é facilmente percebido nas dinâmicas sociais dentro da rede mundial de computadores:

> A revolução da informação favorece o crescimento de tais redes ao tornar possível que atores diversos e dispersos se comuniquem, se consultem, se coordenem e operem em conjunto por grandes distâncias e embasados por mais e melhores informações do que nunca. (NYE, 2011, p.27, tradução nossa)

Essa arquitetura descentralizada tornou a "rede de redes" mais confiável e eficiente, e permitiu o seu crescimento exponencial, com a conexão de mais dispositivos e redes menores, via TCP/IP e outros novos protocolos, até que a internet atingisse a escala atual. Em especial a partir dos anos 90, a popularização de computadores pessoais e de dispositivos móveis levou a internet para o cotidiano de cada vez mais pessoas. Tratou-se de uma expansão acelerada do ambiente informacional, gerando novos setores econômicos, novos espaços de interação social, e também novas preocupações securitárias.

Nye (2011, p.116) aponta que a mudança crucial está na enorme redução dos custos de dispositivos eletrônicos e redes de computadores, a tal ponto que se tornam insignificativas as barreiras à entrada de atores menores no ciberespaço. O número de usuários da rede mundial já alcança 4,9 bilhões de pessoas ao final de 2021, ultrapassando a marca de 60% da população mundial[9]. Quase 54% das pessoas no planeta utilizam alguma plataforma social, e o líder Facebook possui cerca de 2.9 bilhões de usuários ativos[10]. O poder da informação nunca antes esteve tão acessível a um número tão grande de pessoas, e isso significa que "a política mundial não será a província exclusiva dos governos [...] todos os governos terão menos controle de sua agenda." Nye (2011, p.116, tradução nossa).

Conquanto se possa argumentar, como Nye (2011, p.117) o faz[11], que certos tipos de informações, ditas estratégicas ou sensíveis, ainda possuem um alto custo de obtenção e, assim,

[9] Disponível em https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/
[10] Disponível em https://www.statista.com/markets/424/topic/540/social-media-user-generated-content/
[11] "[…] mesmo que a disseminação de informações existentes não custe muito, a coleta e produção de novas informações frequentemente exigem grandes investimentos. Em muitas situações competitivas, as informações novas são as mais importantes. […] A coleta de inteligência é um bom exemplo. EUA, Rússia, Grã-Bretanha, China e França têm capacidades de coleta e produção de inteligência que superam em muito as da maioria dos estados." Nye (2011, p.117, tradução nossa)

estariam mais restritas aos Estados, o presente trabalho arrazoará mais à frente que mesmo essa assimetria tem sido reduzida rapidamente nos últimos anos.

Hoje em dia, muitos outros protocolos, tecnologias e processos estão envolvidos na estrutura da internet. Para que os pacotes digitais possam percorrer o mundo de um servidor de dados até o cliente destinatário, ligações interoceânicas robustas (*backbones*) ou constelações de satélites são necessárias. Em geral, são empresas privadas (os provedores de internet - ISP[12]) que fornecem o serviço de acesso à rede. Instituições internacionais como a ICANN[13] centralizam o controle da nomeação de endereços na rede, de modo a manter a confiabilidade do sistema. Como se vê, muitos dos aspectos da internet possuem uma forte vinculação territorial e política, e podem então ser controlados por meio de formas mais tradicionais de poder.

Este segundo tópico se propôs a apresentar os diferentes espaços ou ambientes onde o poder da informação nas relações internacionais se manifesta. A distinção entre Ambiente Informacional, Ciberespaço e Internet possibilitou visualizar as interações entre eles, viabilizando identificar de que forma a expansão da cibernética aumentou a relevância da informação na política internacional. Outrossim, o conceito de Espaço Cibernético adotado forneceu percepções de como seu alcance global e sua estrutura reticular favorecem atores individuais organizados em redes.

O tópico seguinte intenta expor conceitos de poder aplicados diretamente nos espaços de poder aqui analisados. Nesse sentido, empenhar-se-á em abordar os conceitos de Poder Informacional e Poder Cibernético, presentes na literatura sobre o tema.

[12] Do inglês: *Internet Service Providers*

[13] A *Internet Corporation for Assigned Names and Numbers* controla a atribuição de endereços IP e nomes de domínio (ex: endereços de websites). É uma organização não governamental e sem fins lucrativos, com sede na Califórnia – EUA.

2. 3 O Poder Internacional e Poder Cibernético

Apresentados os espaços onde ocorrem as relações de poder em foco neste trabalho, cabe discutir de que formas o Ambiente Informacional e os seus componentes podem ser fontes de poder nas relações internacionais. Para tanto, será interessante abordar os conceitos de Poder Cibernético e de Poder Informacional, presentes na literatura sobre o tema, e analisar os pontos de aproximação e de distanciamento entre eles.

O Poder Cibernético é analisado por diferentes autores no campo das Relações Internacionais, e os conceitos propostos possuem muitos pontos em comum. Kuehl (2009, p.12) define o Poder Cibernético como "a capacidade de usar o ciberespaço para criar vantagens e influenciar eventos em todos os ambientes operacionais e por todos os instrumentos de poder" (KUEHL, 2009, p.12, tradução nossa). Portanto, uma definição baseada na capacidade de se usar o domínio operacional para influenciar eventos e resultados, e que poderia servir como definição de poder em qualquer um dos cinco domínios. O autor destaca que o Poder Cibernético impacta em todos os instrumentos de poder (Político-Diplomático, Informacional, Militar e Econômico), embora esteja naturalmente mais relacionado ao elemento informacional.

Kuehl (2009, p.12) também identifica duas fontes de Poder Cibernético: A tecnologia *per se*, uma vez que a capacidade tecnológica de um ator é o que define em que medida ele poderá acessar e utilizar o ciberespaço; E os "fatores organizacionais", o que remete à estruturação em rede das instituições modernas. "O Poder Cibernético cria sinergias entre os outros elementos e instrumentos de poder e os conecta de maneira a melhorar todos eles" (KUEHL, 2009, p.13, tradução nossa).

Nye (2011, p.123) traz duas definições para o Poder Cibernético. A primeira, baseada em recursos, informa sobre o uso de infraestrutura, redes e software para obter a superioridade no espaço cibernético, ou seja, dominar a criação e a comunicação de informações eletrônicas. A segunda, comportamental, relaciona poder à capacidade de se obter os resultados preferíveis por meio dos recursos cibernéticos, seja no próprio ciberespaço ou nos demais domínios operacionais. Para o autor, devido a características como o anonimato e o baixo custo de entrada no ciberespaço, o Poder Cibernético é marcado pela maior difusão entre os atores. Indivíduos têm pouco a perder nesse domínio, em comparação com as vulnerabilidades de um Estado cujos sistemas estratégicos estejam altamente informatizados. Essa redução na assimetria entre as capacidades dos diferentes atores seria, portanto, uma fonte de poder internacional:

> As características do ciberespaço reduzem alguns dos diferenciais de poder entre os atores e, assim, fornecem um bom exemplo da difusão de poder que

> caracteriza a política global neste século. É improvável que as maiores potências consigam dominar esse domínio tanto quanto dominam outros, como o marítimo ou o aéreo. Mas o ciberespaço também demonstra que a difusão do poder não significa igualdade de poder ou a substituição dos governos como os atores mais poderosos da política mundial. […] enquanto deixa os governos como atores mais fortes, o domínio cibernético provavelmente verá um **aumento na difusão de poder para atores não estatais** e **a centralidade da rede como uma dimensão-chave do poder** no século XXI. (NYE, 2011, p.150-151, tradução nossa, grifo nosso)

O conceito de Poder Informacional adotado no presente trabalho foi desenvolvido pela cientista da informação Sandra Braman (2006 apud Ávila e Pinheiro, 2014). Em uma das conceituações da autora, a "[...] informação pode ser 'força constitutiva da sociedade', no sentido de que informação molda o próprio contexto" (Ávila e Pinheiro, 2014, p.42). Essa delimitação dialoga com as teorias sistêmicas do poder internacional, e corrobora o argumento de que a informação possui papel estrutural, moldando o sistema e influenciando o comportamento das unidades.

Além disso, o Poder Informacional interage com cada uma das três faces do poder, visto que, para Braman (2006 apud ÁVILA; PINHEIRO, 2014), todas as fontes de poder – recursos materiais, estruturas sociais e símbolos ideacionais – possuem um aspecto informacional em sua gênese. A autora coloca, assim, o Poder Informacional como uma quarta face do poder, para além dos poderes Instrumental (1ª face), Estrutural (2ª face) e Simbólico (3ª face). Portanto, faz sentido pensar em uma estratégia de conversão de poder na qual o agente aplica suas capacidades em uma dimensão que o favorece, com o objetivo de gerar resultado indiretamente em alguma das dimensões restantes:

> "O fluxo de informação que influencia a percepção do público (poder simbólico) pode transformar de forma tão significativa modos de produção (poder instrumental) que práticas organizacionais são alteradas (poder estrutural) de forma a tornar possível reunir e processar outros tipos de informação (poder informacional). O exercício do poder, portanto, na maioria das vezes, envolve um conjunto de estratégias" (BRAMAN, 2006 apud ÁVILA; PINHEIRO, 2014, p.45).

Considerando as definições acima expostas, pode-se inferir uma relação similar àquela proposta entre o Ambiente Informacional e o Espaço Cibernético. Nessa linha de pensamento, o Poder Informacional seria um conceito mais amplo, dentro do qual estariam contidos os aspectos informacionais ligados à eletrônica e ao espectro eletromagnético, que são as fontes do Poder Cibernético. Da mesma forma que a Revolução das TICs transformou o ciberespaço na dimensão dominante do AI, o Poder Cibernético se tornou a principal forma de Poder Informacional exercida no contexto do século XXI.

Adicionalmente, Nye (2011) e Braman (2006 apud ÁVILA; PINHEIRO, 2014) chegam a conclusões similares acerca do impacto da informação em cada uma das faces do poder. Nye (2011) identifica exemplos de Hard e Soft Power em cada uma das três faces, no contexto do espaço cibernético. Em particular, nota-se que os aspectos do poder mais acessíveis a atores não estatais são aqueles relacionados ao Soft Power e às segunda e terceira faces do poder, que são as faces ditas "estruturais".

Tabela 2 - Poder Cibernético em cada uma das faces do poder.

	Primeira Face	**Segunda Face**	**Terceira Face**
	A induzindo B a fazer o que B inicialmente, de outra forma, não faria	A impedindo a escolha de B ao excluir as estratégias de B	A moldando as preferências de B, de modo que algumas estratégias nunca são consideradas por B
Hard:	ataques de negação de serviço, inserção de malware, interrupções de sistemas SCADA, prisões de blogueiros	firewalls, filtros, pressão sobre as empresas para desconsiderarem algumas ideias	ameaças de punir blogueiros que divulgam material censurado
Soft:	campanha de informação para alterar as preferências iniciais dos hackers, recrutamento de membros de organizações terroristas	automonitoramento de ISPs e ferramentas de busca, regras da ICANN sobre nomes de domínio, padrões de software amplamente aceitos	informações para criar preferências (como estímulo ao nacionalismo e a hackers patrióticos), desenvolvimento de normas de repulsa (como pornografia infantil)

Fonte: Elaboração própria, com base em Nye (2011, p.130)

Desse modo, ao dispor de capacidades de enquadramento de agenda e de estabelecimento de preferências, é possível que indivíduos obtenham certos resultados de forma indireta, via transbordamento na face coercitiva, ou via alterações na própria estrutura onde as relações se desenvolvem. Nas palavras de Ávila e Pinheiro (2014), o Poder Informacional

> É um poder racional, que não só alteraria a estrutura social geral na qual os atores se inserem, isto é, os poderes informacionais influenciariam na construção da realidade política e social nas quais as relações acontecem, como também gerariam atitudes e comportamentos específicos. (ÁVILA; PINHEIRO, 2014, p.47)

Um exemplo frequente na literatura, como foi visto, é a construção de narrativas que visem legitimar ou rechaçar as ações de um Estado, influenciar a opinião pública e afetar o moral de combatentes e de civis. "As narrativas são particularmente importantes para enquadrar questões de maneira persuasiva, de modo que alguns 'fatos' se tornem importantes e outros caiam no esquecimento" (NYE, 2011, p.93). O autor também reconhece essa estratégia indireta de conversão de poder, ao afirmar que:

> Mais comum, no entanto, é um modelo de duas etapas no qual o público e terceiros são influenciados e, por sua vez, afetam os líderes de outros países.

> Nesse caso, o soft power tem um importante efeito indireto ao criar um ambiente propício para as decisões. Alternativamente, se um ator ou ação é percebido como repulsivo, cria um ambiente incapacitante. (NYE, 2011, p.94)

Finalmente, Ávila e Pinheiro reconhecem a informação como fonte de poder, tanto em uma conceituação reducionista (informação como um recurso que se possui) quanto em seu aspecto sistêmico (informação como estruturante das relações):

> "Poder informacional também é algo em si mesmo: é, por exemplo, a capacidade de se criar, usar, disseminar e controlar informação. É ainda uma relação de assimetria entre dois atores, onde um pode disponibilizar de mais elementos informacionais que outros e, portanto, passar a dominá-lo" (ÁVILA; PINHEIRO, 2014, p.48).

Esse terceiro tópico buscou abordar os espaços de poder derivado da informação no contexto da Revolução Digital, distinguindo-os (Ambiente Informacional, Ciberespaço e Internet) e relacionando-os. Os impactos desta revolução se disseminaram para outros ambientes e domínios operacionais, visto a ubiquidade do papel da informação no contexto de uma sociedade ultra conectada. Mais importante, as peculiaridades do desenvolvimento tecnológico descentralizado propiciaram o ganho relativo de capacidade por parte de indivíduos e atores não-estatais, complicando as relações políticas internacionais. Assim, a informação vem ganhando relevância como fonte de poder, seja como recurso a ser adquirido e negado, seja por seu uso indireto para se obter os resultados desejados na estrutura ou entre as três faces relacionais, seja ainda pela redução da assimetria entre os atores.

No tópico seguinte, será explorada a Atividade de Inteligência e, mais especificamente, a metodologia da Inteligência de Fontes Abertas. Espera-se elucidar de que maneiras a Revolução das TICs influenciou o método da OSINT, propiciando que atores não estatais se tornassem cada vez mais atuantes nessa atividade.

2. 4 Inteligência de Fontes Abertas – OSINT

A posse de informações relevantes e tempestivas perfaz um aspecto importante do poder estatal e das relações políticas mundiais. A construção de instrumentos de inteligência que assessorem a tomada de decisão não é um fenômeno novo na burocracia estatal, e pode ser considerada um dos objetivos tanto da diplomacia pública quanto da espionagem. Também não é novidade a utilização, em relatórios de inteligência, de informações públicas e amplamente distribuídas, embora a Revolução da Informação tenha gerado novos desafios e possibilidades ao ofício.

Este tópico tem por objetivo apresentar uma visão geral da Atividade de Inteligência e de algumas de suas metodologias, com foco nos procedimentos de coleta de informações. Será explorado o papel das fontes abertas (ostensivas) de informações como matéria-prima na geração de um produto final de inteligência. Por fim, argumentar-se-á que indivíduos e agentes não estatais estão se tornando cada vez atuantes e assertivos na comunidade de inteligência, e que a evolução tecnológica está facilitando o acesso público e em tempo real de informações antes consideradas restritas.

A Atividade de Inteligência é uma função integrante da burocracia do Estado Moderno, envolvendo a coleta de informações e seu posterior tratamento para subsidiar o tomador de decisão. A Inteligência pode ser definida de forma ampla como "toda informação coletada, organizada ou analisada para atender as demandas de um tomador de decisão" (CEPIK, 2003, p.27), isto é, tem como objetivo apoiar a implementação de políticas públicas em áreas como segurança pública, política externa e defesa nacional.

Nesse sentido, "a inteligência se diferencia da mera informação por sua capacidade explicativa e/ou preditiva" (CEPIK, 2003, p.28), o que implica a existência de um processo de transformação dessa informação. Cepik (2003, p.32) identifica as etapas principais desse processo, denominado "Ciclo de Inteligência":

> As descrições convencionais do ciclo da inteligência chegam a destacar até 10 passos ou etapas principais que caracterizam a atividade, a saber: 1) requerimentos informacionais, 2) planejamento, 3) gerenciamento dos meios técnicos de coleta, **4) coleta a partir de fontes singulares**, 5) processamento, 6) análise das informações obtidas de fontes diversas, 7) produção de relatórios, informes e estudos, 8) disseminação dos produtos, 9) consumo pelos usuários e 10) avaliação (feedback). (CEPIK, 2003, p.32, grifo nosso)

Dentro do escopo do presente trabalho, destaca-se a etapa de coleta de informações, feita a partir de fontes singulares. De fato, "as atividades especializadas de coleta absorvem entre 80 e 90% dos investimentos governamentais na área de inteligência nos países centrais"

(CEPIK, 2003, p.35). No contexto da operacionalização da Atividade de Inteligência, tradicionalmente definem-se "disciplinas" especializadas no levantamento de informações por meios e fontes específicas, por exemplo: HUMINT, inteligência de fontes humanas (um eufemismo para espionagem); SIGINT, interceptação e decodificação de sinais eletromagnéticos; IMINT; inteligência obtida por imagens de reconhecimento, principalmente imagens de satélite. No âmbito do Ciclo de Inteligência, a coleta e o processamento de informações são feitos para cada uma dessas fontes singulares, e os resultados são analisados em conjunto na produção de um relatório multi-fonte de inteligência.

Em especial, a chamada Inteligência de Fontes Abertas (OSINT) consiste na utilização de fontes cujo acesso não possui restrições de segurança, como autenticação ou criptografia. Exemplificando, a coleta de informações de fontes abertas pode consistir

> [...] na obtenção legal de documentos oficiais sem restrição de segurança, da observação direta e não clandestina dos aspectos políticos, militares e econômicos da vida interna de outros países ou alvos, do monitoramento da mídia, da aquisição legal de livros e revistas especializadas de caráter técnico-científico, enfim, de um leque mais ou menos amplo de fontes disponíveis cujo acesso é permitido sem restrições especiais de segurança. (CEPIK, 2003, p.51)

A utilização institucional de fontes abertas remonta ao final da Segunda Guerra e início da Guerra fria, com o estabelecimento de agências como a *Foreign Broadcast Intelligence Service* (FBIS) nos EUA e a *BBC Monitoring* no Reino Unido. Inicialmente, grande parte do trabalho consistia apenas em monitorar e traduzir a imprensa estrangeira, de modo que Williams e Blum (2018, p.4) delimitam esta como a OSINT de primeira geração. Entretanto, a Revolução das TICs trouxe mudanças fundamentais na natureza e na quantidade de dados abertos disponíveis. Nas palavras de Mercado (2004, p.47):

> A revolução na tecnologia da informação, no comércio e na política desde o fim da Guerra Fria está apenas tornando as fontes abertas mais acessíveis, onipresentes e valiosas. Simplificando, pode-se reunir mais inteligência aberta com maior facilidade e com menor custo do que nunca. A explosão da OSINT está transformando o mundo da inteligência com o **surgimento de versões abertas** das artes secretas da inteligência humana (HUMINT), imagens aéreas (IMINT) e inteligência de sinais (SIGINT). (MERCADO, 2004, p.47, tradução nossa, grifo nosso)

Essas mudanças trazem a chamada OSINT de segunda geração, segundo Williams e Blum (2018, p.4), o que implica em um trabalho mais extensivo nas etapas de aquisição e de processamento dos dados. Além de conteúdo gerado por instituições, como transmissões de televisão e de rádio e publicações editoriais, um grande volume de conteúdo gerado por indivíduos passa a fazer parte do material ostensivo a ser analisado. "A OSINT de segunda geração evoluiu em grande parte devido à Web 2.0 – uma mudança no contexto da internet para

páginas da web dinâmicas e conteúdos gerados pelo usuário." (WILLIAMS; BLUM, 2018, p.39, tradução nossa)[14], e pode-se citar, a título de exemplo, o conteúdo publicado em plataformas sociais como Facebook, Twitter, VKontakte e Weibo.

Outrossim, esse novo conteúdo possui peculiaridades que dificultam a automatização do tratamento de dados, como o uso intenso de gírias, a baixa preocupação com erros de digitação e a predominância de imagens e de vídeos no conjunto dos conteúdos compartilhados. Em contraste, o tratamento de informações da primeira geração foi facilitado pela evolução de ferramentas automáticas de tradução, de conversão áudio-texto e de reconhecimento de caracteres (OCR)[15].

Com relação ao tipo de conteúdo publicizado nessas plataformas sociais, chama a atenção aquele divulgado em forma de imagens ou de vídeos, visto que possuem um valor probatório intrínseco:

> Na era da informação, a imagem tem uma "superioridade relativa" sobre o texto escrito, especialmente porque, dentro da cultura visual, tende a ser reproduzida e consumida com maior rapidez e eficiência logística, atendendo melhor à difusão de discursos e criação de sentidos. (BERGER, 1987 apud KLANOVICZ, 2006, p. 66).

Constata-se, portanto, de que maneira a segunda geração de OSINT possibilitou a inserção de indivíduos e atores não estatais na Atividade de Inteligência. Essa comunidade, cujos participantes por vezes não possuem nenhuma vinculação institucional, passou a ter acesso a um amplo leque de fontes ostensivas de segunda geração, como postagens em redes sociais, fóruns e grupos de mensagens instantâneas. "Fica óbvio que a grande vantagem das fontes abertas é o alto grau de oportunidade e o baixo custo para obtê-las." (AFONSO, 2006, p.56). Na mesma linha de pensamento, Mercado (2004) afirma que

> Coletar informações hoje em dia é, às vezes, menos uma questão de se esgueirar por becos escuros em uma terra estrangeira para encontrar algum agente secreto, do que uma questão de navegar na Internet sob as luzes fluorescentes de um cubículo de escritório para encontrar alguma fonte aberta. (MERCADO, 2004, p.45, tradução nossa)

Mormente, além desse acesso facilitado a conteúdos gerados por indivíduos, a Revolução das TICs popularizou certos tipos de informações cuja aquisição era proibitivamente custosa, como por exemplo imagens de satélite e imagens de campo. Não só se tornou possível visualizar qualquer ponto do globo por meio de plataformas como Google Earth[16], mas também

---

[14] Os autores propõem, ainda, as características de uma possível terceira geração de OSINT, marcada por transmissões ao vivo e pela pervasividade de dados encriptados.
[15] Do termo em inglês: *Optical Character Recognition*
[16] Outras plataformas similares incluem: *Sentinel Hub Playground*; *Zoom Earth*; *World Imagery Wayback*.

a qualidade e a frequência de atualização das imagens em pontos de interesse aumentaram significativamente nos últimos anos. Mesmo tecnologias antes restritas aos militares estão hoje ao alcance de qualquer um com uma conexão à internet, como por exemplo imagens de radar SAR[17] obtidas por satélites, que permitem imagens noturnas, "enxergar" através de nuvens e instabilidades climáticas, e até visualizar submarinos até uma certa profundidade. Nesse sentido, "ao ressaltarmos a importância da OSINT, chamamos a atenção para o aumento da quantidade das fontes abertas, assim como do acesso público a muitos dados que antes eram negados [...]" (AFONSO, 2006, p.60).

Cabe mencionar, ainda, que as Fontes Abertas não são necessariamente sinônimo de "fontes gratuitas". É colocado, no presente trabalho, que grande parte das informações disponíveis gratuitamente em redes sociais e aplicativos de imagens de satélite fornecem dados sensíveis e tempestivos acerca de diversos eventos de interesse. Não obstante, também está disponível comercialmente uma gama de tecnologias de obtenção de dados, como as imagens SAR, para aqueles atores não estatais dispostos a pagar por esse acesso. Tais recursos também podem ser considerados OSINT, a depender do entendimento acerca das barreiras à obtenção desses dados. Sendo o acesso comercial considerado parte integrante dos meios utilizados na OSINT, percebe-se que atores que disponham dos recursos necessários podem expandir o tipo de dados a que têm acesso:

> OSINT é a exploração analítica de informações que estão legalmente disponíveis e no domínio público. Ou seja, não são adquiridas clandestinamente por meio de espionagem ou meios ilegais, nem "restritas" ao público por sensibilidade governamental ou comercial. (GIBSON, 2004, p.19, tradução nossa)

Esse quarto e último tópico do capítulo teórico objetivou apresentar a Atividade de Inteligência como uma atividade tradicional da burocracia estatal. Dentro da etapa de coleta de informações, destacou-se a OSINT como uma metodologia que vem sendo consideravelmente impactada pela Revolução Digital e pela expansão do Ciberespaço. A disseminação de dispositivos móveis, das redes sociais e o aumento do alcance da internet oportunizaram aos atores não estatais o acesso a um conjunto crescente de fontes ostensivas, quase imediatamente

[17] O Synthetic-Aperture Radar (SAR) é uma forma de radar usada para criar imagens bidimensionais ou reconstruções tridimensionais de objetos, como paisagens. Essa tecnologia usa o movimento da antena do radar sobre uma região alvo para fornecer uma resolução espacial mais fina do que os radares convencionais de varredura de feixe estacionário. O SAR é capaz de sensoriamento remoto de alta resolução, independente da altitude de voo e independente do clima, pois pode selecionar frequências para evitar a atenuação do sinal, e possui capacidade de imagem diurna e noturna. As imagens SAR têm amplas aplicações em sensoriamento remoto e mapeamento de superfícies da Terra, inclusive em um contexto de vigilância militar. Fonte: https://www.capellaspace.com/data/why-sar/

após serem produzidas. Essas novas informações não somente são criadas e publicadas em grande quantidade, mas também contêm informações que até recentemente eram negadas a esses atores menores, o que implica em uma maior capacidade informacional.

2. 5 Conclusões parciais

O presente capítulo tencionou estabelecer uma fundamentação teórica acerca da Informação e da Cibernética como elementos de poder empregado pelos diferentes atores da política internacional. O objetivo foi constituir as bases que sustentarão o estudo de caso no capítulo seguinte.

Ao investigar a literatura sobre o tema, foi possível elencar diferentes conceituações do poder da informação, identificar suas convergências e divergências, e depreender as aproximações teóricas que melhor capturam a complexidade do sistema internacional no século XXI. Seja por uma abordagem reducionista, sistêmica ou comportamental, foi possível entender as maneiras pelas quais a informação é fonte de poder nas relações internacionais. Também intentou-se evidenciar o papel emergente dos atores não estatais nessas relações de poder. Finalmente, discorreu-se sobre a Atividade de Inteligência e uma de suas metodologias de coleta de dados, a OSINT, argumentando que esse campo de atuação vem sendo explorado por indivíduos e grupos de indivíduos, em suas relações de poder com as demais unidades do sistema.

Mediante o exposto, torna-se interessante investigar, no caso concreto, de que forma esses novos atores obtêm informações de fontes abertas e aplicam a inteligência gerada a partir delas. Nesse contexto, o recente conflito entre Rússia e Ucrânia se destaca pelo intenso uso de OSINT, tanto pela cobertura da mídia quanto por organizações de verificação de fatos e de combate à desinformação[18].

No capítulo seguinte, este trabalho propõe um estudo de caso referente à invasão militar russa ao território ucraniano no início de 2022. Comparando fontes governamentais e os relatórios de inteligência produzidos pela comunidade OSINT, espera-se elucidar a influência destes atores nas narrativas sobre o evento, bem como argumentar que tal influência se encaixa em certas definições de poder vistas anteriormente.

[18] Exemplos de artigos jornalísticos sobre a utilização de OSINT no conflito: https://www.buzzfeednews.com/article/peteraldhous/osint-ukraine-war-satellite-images-plane-tracking-social e https://www.economist.com/briefing/2022/02/18/a-new-era-of-transparent-warfare-beckons

3 ESTUDO DE CASO

O presente capítulo tem por objetivo exemplificar a utilização de Fontes Abertas em um estudo de caso. Para tanto, buscar-se-á justificar a escolha das relações recentes entre Rússia e Ucrânia, que resultaram em conflitos territoriais a partir de 2014 e culminaram no conflito armado iniciado neste ano de 2022. Intenta-se validar ou falsear, no caso concreto, os elementos colocados na hipótese e na pergunta de pesquisa que norteiam este trabalho: que há uma tendência de aumento da disponibilidade de informações estratégicas, via Ciberespaço e Fontes Abertas; que tal tendência potencializa a ação de atores não estatais em um cenário de conflito internacional; e que tais atores estão se tornando capazes de exercer poder efetivo e alcançar resultados palpáveis na política internacional.

Foi selecionado um evento pregresso, a presença de militares russos nas regiões separatistas do Donbas, de modo a estabelecer um parâmetro de comparação temporal no que diz respeito à utilização de OSINT. A finalidade de tal comparação é identificar algumas mudanças ocorridas no contexto das Fontes Abertas nos últimos anos, como evoluções qualitativas nas tecnologias e nos dados disponíveis.

Por fim, será colocado o caso da invasão do território ucraniano pela Rússia em 2022, focando na mobilização das forças terrestres russas nos dias imediatamente antes ao evento. A intenção é exemplificar de que maneiras a OSINT foi utilizada por atores não estatais para contrapor a narrativa construída pelo Kremlin. Neste momento serão contrapostas fontes oficiais do governo russo, como notas publicadas no site do Ministério da Defesa e no site da presidência, a relatórios contemporâneos produzidos por entidades não estatais que utilizam Fontes Abertas. Para representar a visão geral dessa rede online de colaboradores que é a comunidade OSINT, serão apresentadas duas organizações de destaque nessa área: Bellingcat e CIR.

Espera-se que os dados levantados permitam inferir de que forma as Fontes Abertas foram utilizadas para contestar a narrativa estatal russa, isto é, para restringir o controle que a Rússia tentou exercer sobre a agenda internacional. Adicionalmente, tenciona-se demonstrar o tipo de informação que é possível obter por OSINT, de forma tempestiva, em uma situação de conflito como o caso estudado.

3. 1 Considerações Iniciais

Rússia e Ucrânia são dois países intimamente ligados por relações históricas, culturais, políticas e econômicas. Ambos os países compartilham a mesma origem na etnia Rus, referente a povos que, na Idade Média, habitavam regiões hoje pertencentes a Rússia, Ucrânia e Bielorrússia. Além disso, ambos fizeram parte da União das Repúblicas Socialistas Soviéticas (USRR), desde sua fundação até a dissolução no início dos anos 1990.

A despeito dessas e de outras proximidades, a relação entre Rússia e Ucrânia tem sido caracterizadas por uma situação de conflito latente. Focando no período após a dissolução da USRR, Mielniczuk (2006, p.225-227) afirma que os países estão envolvidos em disputas em diferentes esferas, como conflitos identitários, econômicos e militares.

Na esfera identitária, o governo Russo utiliza a numerosa diáspora russa para pressionar a tomada de decisões ucraniana. Cerca de 17% da população ucraniana se declara etnicamente russa[19], estando esses grupos localizados principalmente nas regiões de fronteira entre os dois países.

Na esfera econômica, o autor cita a dependência ucraniana do gás russo. A região do Dnieper-Donetsk, cujo controle é disputado pelo governo ucraniano e por separatistas apoiados pela Rússia, concentra 90% da produção de gás natural do país[20]. Embora a Ucrânia não importe gás natural diretamente da Rússia desde 2014, o país adquire gás russo por intermédio de revendedores ocidentais, e a rede de gasodutos do país é utilizada para transporte de gás entre Rússia e Europa[21].

Na esfera militar, a presença russa na região da Transnístria (território separatista da Moldávia, no leste europeu) e o interesse ucraniano em se integrar à Organização do Tratado do Atântico Norte OTAN constituem fontes de instabilidade entre os dois países. Conforme apontado por Mielniczuk (2006),

> A participação russa na guerra da Moldávia – que ocorre na fronteira ocidental da Ucrânia – demonstra a disposição da Rússia em garantir pela força seus interesses no "estrangeiro próximo". [...] Além disso, a Ucrânia procura integrar-se à OTAN, o que é visto pela Rússia como um ato de provocação, uma vez que a Rússia não aceita a expansão da Aliança para os países do leste

[19] Exemplos de artigos jornalísticos sobre a utilização de OSINT no conflito: https://www.buzzfeednews.com/article/peteraldhous/osint-ukraine-war-satellite-images-plane-tracking-social, https://www.economist.com/briefing/2022/02/18/a-new-era-of-transparent-warfare-beckons e https://observers.france24.com/en/europe/20220211-meet-the-anonymous-internet-investigators-tracking-russian-movements-on-the-ukrainian-border.

[20] Disponível em https://www.eia.gov/international/overview/country/UKR

[21] Disponível em https://www.reuters.com/business/energy/ukraines-energy-options-limited-event-russian-gas-disruption-2022-02-24/

> europeu. Mas os conflitos mais intensos ocorrem por causa do estatuto de Sevastopol e da divisão da Frota do Mar Negro. (MIELNICZUK, 2006, p.226)

Mais recentemente, a Rússia tem se envolvido em uma série de conflitos interestatais cuja característica marcante é a utilização de meios cibernéticos. De acordo com Connel e Vogler (2017, p.3), os russos enxergam o conflito cibernético por uma lógica mais ampla que suas contrapartes ocidentais, colocando as Operações Cibernéticas (CyberOps) no mesmo nível de outros tipos como Operações Psicológicas (PsyOps) e Informacionais (InfOps), dentro de um contexto holístico de conflito informacional. "Em outras palavras, o meio cibernético é considerado um mecanismo para permitir que o Estado domine o cenário da informação, que é considerado um domínio de guerra por si próprio" (CONNEL; VOGLER, 2017, p.3, tradução nossa). Tais meios foram utilizados tanto de forma isolada quanto coordenada a meios cinéticos, com objetivos diversos, dentre os quais destacam-se campanhas de informação e desinformação, de construção de narrativas e de influência da opinião pública. "A ofensiva cibernética é, assim, relegada a um papel coadjuvante – embora significativo – de ajudar o Estado a alcançar o domínio da informação em todos os estágios do conflito" (CONNEL; VOGLER, 2017, p.5, tradução nossa).

Considerando essa abordagem peculiar quanto aos conflitos cibernéticos, a literatura sobre o tema tem se debruçado sobre os recentes eventos na Estônia, na Geórgia e na Ucrânia, nos quais o embate no domínio cibernético-informacional obteve destaque.

No ano de 2007, em resposta à alteração do local de uma estátua de um soldado soviético no centro de Tallinn, a Estônia sofreu um massivo ataque de Negação de Serviço Distribuída (DDoS[22]), no que pode ser considerado "o primeiro uso coordenado e em larga escala de cibernética pela Rússia para afetar um resultado estratégico em um estado vizinho" (CONNEL; VOGLER, 2017, p.13, tradução nossa). Embora não se possa estabelecer indubitavelmente a autoria desses ataques DDoS, eles certamente exerceram pressão em favor da posição russa, e ocorreram concomitantemente ao congelamento das relações diplomáticas e à imposição de sanções econômicas por parte do Kremlin:

> Ao perturbar e possivelmente desequilibrar o governo e a sociedade estonianos, 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. (BLANK, 2017, p.86, tradução nossa)

Em 2008, a Geórgia se tornou o próximo alvo da atividade russa no espaço cibernético. Após a escalada de tensões entre os dois países acerca das regiões separatistas e pró-Rússia da

[22] Do inglês, *Distributed Deny of Service*

Ossétia do Sul e da Abecásia, o conflito foi deflagrado com a intervenção das forças armadas ossetas e a subsequente resposta militar russa. CyberOps contra os meios de comunicação georgianos, tanto oficiais quanto privados, foram conduzidas em paralelo à entrada de tropas russas nos territórios separatistas. Nesse evento, foi possível identificar a coordenação de capacidades cibernéticas com incursões militares tradicionais:

> Na Geórgia, a Rússia tentou pela primeira vez combinar ataques cinéticos e cibernéticos. Por um lado, contra sistemas de comando-e-controle e de armas, e, por outro lado, ataques psicológicos e de informação contra a mídia, comunicações e percepções. Em outras palavras, a Rússia integrou organicamente o que fontes ocidentais considerariam ataques cibernéticos em uma ampla operação militar e de informações. (BLANK, 2017, p.88, tradução nossa)

Nesse contexto de conflitos marcados por uma forte atuação no espaço cibernético, é possível identificar eventos em que a Inteligência de Fontes Abertas foi utilizada por atores não estatais na verificação de fatos e de incidentes em campo. A expansão da internet, das plataformas sociais e do imageamento por satélite permitiu com que entusiastas geograficamente dispersos se organizassem em comunidades online e passassem a coletar dados públicos, analisando-os segundo uma lógica de *crowdsourcing*[23]:

> A interconexão global e o surgimento de "reportagens lideradas por cidadãos" trouxeram à tona uma nova casta de analistas: a rede de inteligência de *crowdsourcing*, com o objetivo de aproveitar o trabalho de ativistas digitais com ideias semelhantes para desafiar e combater as narrativas estatais. (ÜNVER, 2018, p.14, tradução nossa)

Entre essas comunidades de inteligência, pode-se destacar a Bellingcat[24], um coletivo independente de jornalismo que tem utilizado OSINT na verificação de uma variedade de eventos internacionais. Desde suas origens como um *blog* criado pelo jornalista britânico Eliot Higgins, a organização atingiu notoriedade após uma série de relatórios investigativos acerca de incidentes relacionados ao conflito entre Rússia e Ucrânia. Por exemplo, pode-se citar as investigações acerca da derrubada do voo civil Malaysia Airlines MH17 em julho de 2014, por um míssil terra-ar, enquanto atravessava o território da região separatista de Donetsk. A apuração da Bellingcat utilizou Fontes Abertas para atribuir a autoria aos grupos separatistas pró-Rússia na região, que teriam utilizado armamento militar russo (sistema de mísses Buk)[25].

[23] Colaboração coletiva, em tradução livre do inglês.
[24] Outras comunidades também têm obtido destaque na utilização de OSINT para verificar incidentes de política internacional, violações de direitos humanos, etc. Como exemplo, pode-se citar: Forensic Architecture, Centre for Information Resilience (CIR), entre outros.
[25] Disponível em https://www.bellingcat.com/app/uploads/2015/10/MH17-The-Open-Source-Evidence-EN.pdf

Outro trabalho de destaque do grupo investigou o envenenamento em 2020, por um agente químico, do líder da oposição russa, Alexey Navalny[26].

Não se pode deixar de registrar o viés pró-Ocidente das investigações realizadas pela Bellingcat. Entretanto, espera-se que a objetividade dos dados utilizados pela organização, como imagens de satélite e fotos de redes sociais, permita uma análise que atinja os objetivos propostos neste trabalho, com a ciência de que certos elementos podem ter sido deliberadamente excluídos.

No presente trabalho, será apresentada a investigação da Bellingcat acerca da presença não oficial de tropas russas nos territórios separatistas ucranianos de Donetsk e Lugansk, no ano de 2014. Embora não esteja no escopo deste trabalho realizar um aprofundamento no estudo desses eventos específicos, propõe-se uma breve apresentação dos mesmos, com foco na tempestividade dos dados disponíveis e nas tecnologias utilizadas para a coleta de dados abertos. O objetivo é identificar uma tendência de aumento da disponibilidade de dados e de tecnologias sensíveis, quando comparados com os eventos deste ano de 2022.

[26] Disponível em https://www.bellingcat.com/resources/2020/12/14/navalny-fsb-methodology/

3. 2 Os eventos na Criméia e no Donbas

A chamada Revolução da Dignidade ucraniana teve início em novembro de 2013, com a decisão unilateral do governo Ianukóvytch de atrasar a assinatura de um acordo de aproximação com a União Europeia (UE). A dura repressão policial a protestos pacíficos em Kiev gerou uma forte resposta da sociedade, culminando em uma onda de protestos que ficariam conhecidos como Euromaidan. O objetivo dos protestantes escalou a partir de então, passando da busca pela retomada do curso de integração com a UE para a renúncia do governo e de seu gabinete, vistos como ilegítimos e não representativos dos interesses da população (SHVEDA; PARK, 2016, p.87). Os protestos levaram à queda do governo e à convocação de novas eleições no ano de 2014, conduzidas no mesmo contexto em que ocorria a anexação da península da Crimeia pela Rússia, e que separatistas pró-Rússia iniciavam o conflito armado pelo controle dos territórios de Donetsk e Lugansk.

A presença de militares russos na região do Donbas e o suporte oficial às repúblicas autoproclamadas foram inicialmente negados pelo Kremlin (BELLINGCAT, 2015). Em mais de uma oportunidade, o presidente russo Vladmir Putin rejeitou qualquer envolvimento direto do país no teatro de operações no leste da Ucrânia[27], posição corroborada por outras autoridades do governo.

Nesse contexto, a Bellingcat publicou, no ano de 2015, um relatório investigando possíveis locais de transposição da fronteira entre Rússia e Ucrânia, apontando o surgimento de novas estradas entre os países, principalmente na área rural. Neste relatório, foram utilizadas imagens de satélite comuns, obtidas via Google Earth e Digital Globe[28], bem como fotos e vídeos publicados em plataformas como Youtube, Twitter e VKontakte. Os dados analisados no relatório cobrem o período de julho a setembro de 2014, compreendendo um ponto de inflexão entre o que parecia ser uma retirada das forças separatistas e o aumento da intensidade dos confrontos, com os separatistas obtendo ganhos territoriais significativos. Alegadamente, os combatentes separatistas foram reforçados por militares russos neste período (BELLINGCAT, 2015, p.6).

O relatório mencionado identifica diversas travessias de fronteira que não existiam antes do período analisado, ou que apresentam sinais de aumento de tráfego neste período. Essas

---

[27] Disponível em https://www.telegraph.co.uk/news/worldnews/vladimir-putin/12054164/Vladimir-Putins-annual-press-conference-2015-live.html

[28] As empresas DigitalGlobe e MDA Holdings Company se fundiram sob o nome Maxar Technologies em Outubro de 2017. Fonte: https://www.geospatialworld.net/news/mda-dg-combined-entity-to-be-rebranded-as-maxar-technologies/

travessias se encontram próximas a regiões onde ocorreram intensos conflitos durante o período analisado, e próximas a acampamentos militares russos, em território russo, identificados por imagens de satélite.

Figura 1 - Surgimento de nova travessia de fronteira.

Figure 5: Border traffic near Severnyi (48.352967, 39.942758): top left: 27 April 2013; top right: 15 May 2014; bottom left: 8 August 2014; bottom right: 31 August 2014; source: Google Earth

Fonte: Bellingcat (2015)

Por exemplo, a sequência de imagens abaixo exibe uma mesma região em três momentos diferentes: Antes do início do conflito armado, em outubro de 2013; e em dois momentos durante o verão de 2014. A linha amarela corresponde à fronteira entre Ucrânia, ao norte, e Rússia, ao sul. É possível identificar a abertura de uma estrada atravessando a fronteira, e de um pequeno acampamento em território ucraniano, com a presença de alguns veículos. A imagem mais recente indica que a frequência de uso da estrada e do acampamento aumentou nesse período. Segundo a Bellingcat (2015, p.26), o governo dos EUA reportou ataques a posições ucranianas nessa região. Adicionalmente, foram identificados acampamentos militares russos próximos a essa estrada, em território russo, por meio de imagens postadas na plataforma social VKontakte em agosto de 2014[29].

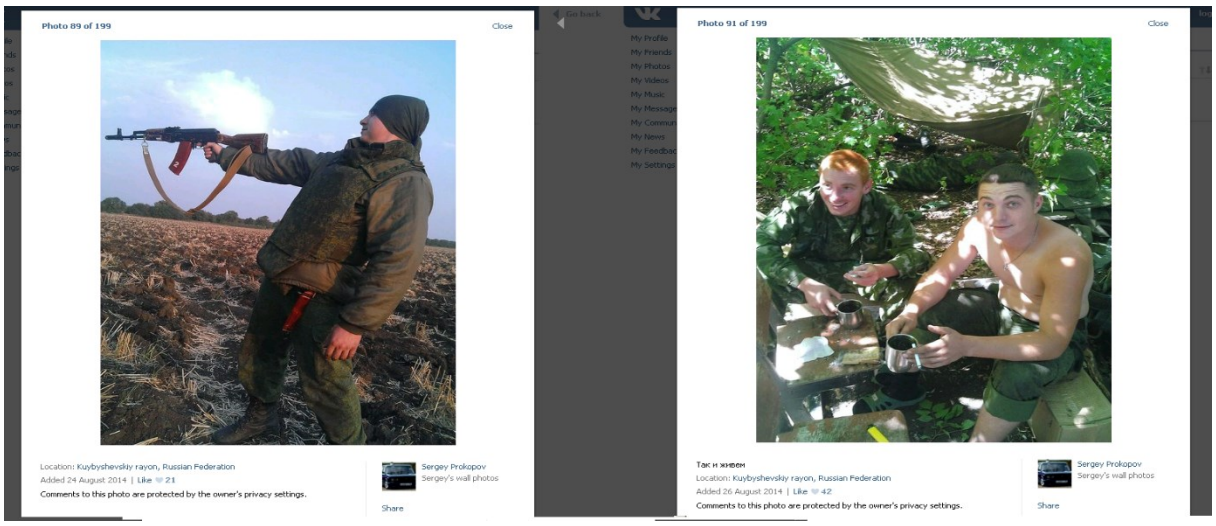
[29] O relatório da Bellingcat não apresenta uma verificação da localização das imagens, que foi adicionada pelos próprios usuários na rede social.

Figura 2 - Surgimento de nova travessia de fronteira.

Figure 22: Border crossing north of Novaya Nadezhda (47.869858, 39.068522): comparison of 12 October 2013 (left), 4 August 2014 (middle), and 15 August 2014; the area of the border crossing and a camp near the crossing are enlarged; contrast and tone adjusted to ease identification for the August imagery; course of border added manually; source: preview imagery from TerraServer

Fonte: Bellingcat (2015)

Figura 3 - Fotos de soldados russos na região do conflito.



Fonte: Bellingcat (2015)

Nota-se que, à época, não foram utilizados recursos como imagens por satélite com a tecnologia SAR, que possuem certos benefícios sobre as imagens comuns, como citado anteriormente. A despeito de algumas imagens coletadas pela Bellingcat estarem obstruídas por fenômenos climáticos, como nuvens, elas ainda sim foram consideradas fontes utilizáveis como evidência no relatório. No exemplo abaixo, a sequência temporal de imagens por satélite de um acampamento militar russo foi prejudicada por esse motivo. Infere-se, portanto, que atores não

estatais ainda possuíam, naquele momento, certa dificuldade de acessar esta e outras tecnologias mais avançadas.

Figura 4 - Exemplo de imagem de satélite obstruída por nuvens.

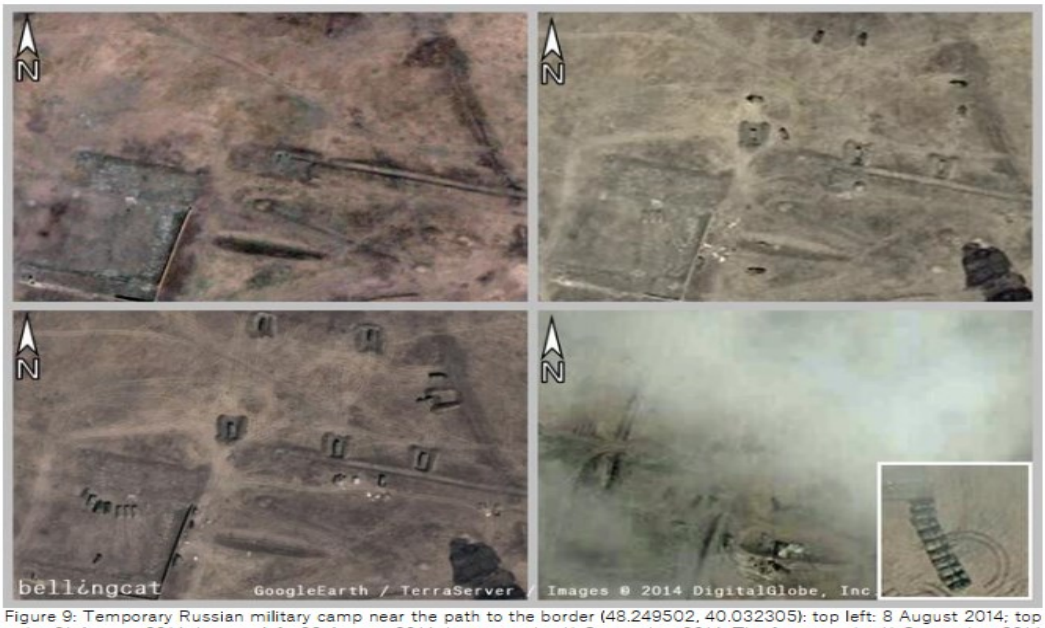


Figure 9: Temporary Russian military camp near the path to the border (48.249502, 40.032305): top left: 8 August 2014; top right: 21 August 2014; bottom left: 22 August 2014; bottom right: 11 September 2014. The frame in the 11 September 2014 imagery shows a group of vehicles 250 meters west of the camp (48.249723, 40.028027); contrast and tone adjusted; sources: Google Earth (8 August and 22 August), preview imagery from TerraServer (21 August and 11 September)

Fonte: Bellingcat (2015)

Ademais, percebe-se que predominam no relatório a análise de imagens estáticas, embora alguns vídeos também sejam utilizados como fonte. Os dados utilizados como referência na argumentação da Bellingcat são citados em links nas notas de rodapé no relatório, totalizando 173 links. Destes, apenas 11 são vídeos, em sua maioria publicados na plataforma Youtube. No presente estudo, notou-se também que muitos desses vídeos apresentados no relatório não estão mais disponíveis para visualização. É possível que o material tenha sido retirado do ar por apresentar conteúdo sensível ou explícito, ou que tenha sido removido pelos próprios usuários que as enviaram.

Por fim, cabe uma análise acerca da tempestividade com que os dados se tornaram disponíveis abertamente na internet. Conforme mencionado, o relatório cobre eventos ocorridos entre julho e setembro de 2014. Trata-se de uma consolidação das análises dos dados disponíveis online até a data da publicação. Nenhuma das postagens da própria Bellingcat que foram referenciadas no relatório é datada de 2014. Embora utilizem material cuja disponibilização ocorreu em datas próximas aos eventos, como as imagens e vídeos publicados em plataformas sociais, tais dados somente foram coletados e analisados pela Bellingcat alguns

meses mais tarde. Isso pode indicar uma dificuldade em se obter e verificar rapidamente, naquele momento, dados de Fontes Abertas.

O caso da presença de tropas russas na região do Donbas foi apresentado com o objetivo de exemplificar as possibilidades que a OSINT fornece a atores não estatais. Em especial, buscou-se destacar certas limitações da investigação à época dos fatos, no que tange às tecnologias e aos dados disponíveis. Será visto no caso seguinte que a continuidade da evolução da cibernética reduziu significativamente, e em um curto período, muitas dessas limitações.

3. 3 A invasão da Ucrânia em 2022

Nesse sentido, o presente trabalho se propõe a apresentar o papel da OSINT no recente conflito armado entre Rússia e Ucrânia, deflagrado no final de fevereiro de 2022. De modo a delimitar o escopo do estudo de caso, optou-se pela análise da mobilização das forças armadas russas no contexto da operação "Union-Courage" e de outros exercícios militares na fronteira entre os países. O enfoque será no período imediatamente anterior à invasão do território ucraniano, isto é, nos meses de janeiro e fevereiro deste ano.

Será apresentada a narrativa oficial russa a respeito de tais mobilizações, por meio de declarações publicadas pelo Ministério da Defesa e pelo site do Kremlin (presidência). Essa narrativa, no período analisado, se concentra em dois pontos fundamentais: que os exercícios militares na região possuem natureza puramente defensiva, e que as tropas iniciaram a desmobilização na data prevista para o encerramento das atividades conjuntas. Artigos de cunho jornalístico e declarações de autoridades em entrevistas e pronunciamentos serão utilizados de forma complementar, quando cabível.

Em contrapartida, será apresentada o monitoramento, por atores não estatais utilizando Fontes Abertas, da movimentação das tropas russas. Esse monitoramento será analisado por meio dos relatórios de conjuntura publicados pelo "Centre for Information Resilience". A intenção é apontar qual tipo de conhecimento foi possível construir utilizando-se da OSINT, naquele momento, e exemplificar como esse ator foi capaz de confrontar a narrativa russa, de fato limitando o controle do Kremlin sobre a agenda internacional.

3. 2. 3 Concentração e deslocamento de tropas

A partir de dezembro de 2021, e ao longo de janeiro e fevereiro de 2022, governos e a mídia ocidentais passaram a destacar com maior frequência a acumulação de forças russas próximo às fronteiras entre Rússia, Belarus e Ucrânia.

O governo russo, por sua vez, afirmou que a presença de ativos militares na região se devia a um exercício militar conjunto entre o país e Belarus[30]. Chamado de "Union-Courage 2022", o exercício iniciou em 10 de fevereiro de 2022, com a previsão de duração de dez dias, apenas. O exercício envolveu a transferência de pessoal e de equipamentos por mais de dez mil quilômetros[31], o que significa a presença de grupos antes empregados nas regiões mais orientais

[30] Disponível em https://eng.mil.ru/en/news_page/country/more.htm?id=12407977
[31] Disponível em https://eng.mil.ru/en/news_page/country/more.htm?id=12406871

do país. Segundo o Ministério da Defesa da Rússia, unidades militares do Distrito Militar do Leste estariam presentes nas atividades executadas em Belarus. Ademais, o Union-Courage teria como objetivos, oficialmente, fortalecer a proteção das fronteiras estatais contra a infiltração de grupos armados, bloquear canais de entrega de armamentos e de munição, simular a detecção de grupos de reconhecimento e sabotagem inimigos, entre outros.

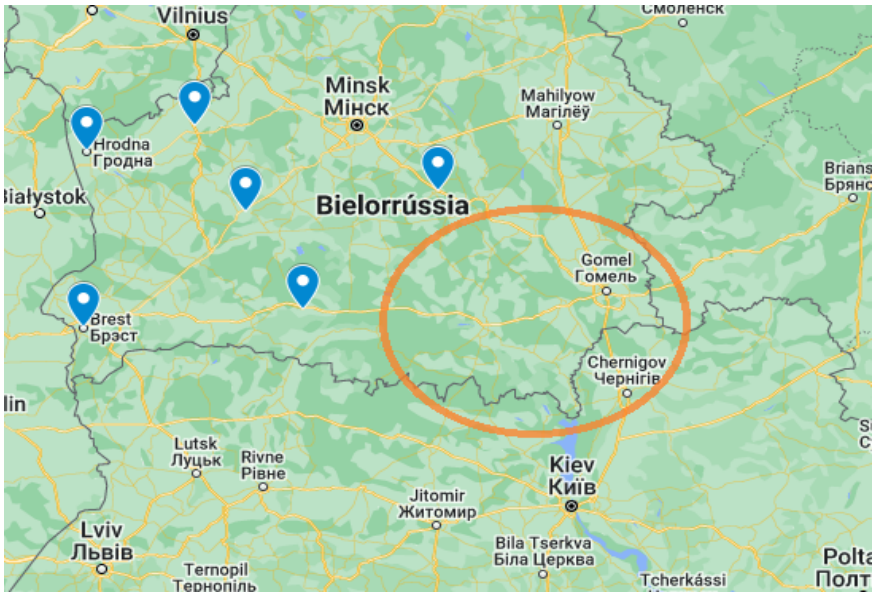
Não obstante ter sido a maior concentração de militares russos em território belarusso desde o final da Guerra Fria[32], o Kremlin afirma se tratar de uma operação meramente defensiva. É importante citar que outras operações militares também estavam ocorrendo simultaneamente, no sul da Rússia e na península da Crimeia[33], ambas regiões de fronteira com a Ucrânia. A figura 8 mostra os locais de execução do exercício Union-Courage, conforme indicados pelo Ministério da Defesa russo. É interessante destacar que as bases de operações divulgadas estão relativamente distantes da fronteira com a Ucrânia. Em especial, a imagem oficial indica que as atividades evitariam a região da fronteira que fica mais próxima à capital ucraniana, Kiev, deixando uma espécie de vazio geográfico.

Figura 5 - Mapa indicando os pontos de interesse da operação "Union-Courage 2022", em território belarusso.

Fonte: Ministério da Defesa da Rússia[34]

[32] Disponível em https://www.reuters.com/world/europe/russia-has-sent-some-30000-combat-troops-modern-weapons-belarus-nato-says-2022-02-03/
[33] Disponível em https://www.bbc.com/news/world-europe-60158694
[34] Disponível em https://eng.mil.ru/en/mission/practice/all/rehimost-2022.htm

Figura 6 - Vazio geográfico entre os locais oficiais de atividades do Union-Courage e a capital Kiev.



Fonte: elaborado pelo autor

Essa concentração de tropas gerou preocupações no ocidente, em especial nos países bálticos, nos países-membros da OTAN, e, naturalmente, na própria Ucrânia. Esta mobilização russa foi qualificada pela organização como "não provocada" e "injustificada"[35]. Em 16 de fevereiro, os ministros da defesa dos países da OTAN se reuniram em Bruxelas para "abordar a contínua concentração militar da Rússia dentro e ao redor da Ucrânia"[36]. Nesse encontro, o secretário geral da organização, Jens Stoltenberg, afirmou que não havia, até o momento, sinais de desmobilização, e que a Rússia possuía uma força massiva e com capacidades de ponta nas regiões próximas à fronteira com a Ucrânia.

Próximo à data prevista para o encerramento do Union-Courage, mais especificamente nos dias 17 e 18 de fevereiro, o governo russo começou a publicizar que parte de seus ativos militares na região estava sendo "transferida para seus pontos de mobilização permanente"[37]. Isto é, as unidades militares, incluindo unidades de blindados[38,39], estariam se retirando do território de Belarus e de outras regiões próximas à fronteira ucraniana, e marchando de volta às suas bases de origem. Declarações similares foram feitas a respeito do deslocamento de

[35] Disponível em https://www.nato.int/cps/en/natohq/official_texts_191931.htm
[36] Disponível em https://www.nato.int/cps/en/natohq/opinions_191839.htm. Destaca-se que, durante a entrevista, um repórter questionou ao Secretário Geral da Otan sobre o porquê de se acreditar nas palavras da organização, ao invés das alegações russas de que as tropas já estariam iniciando a desmobilização, ao que lhe foi respondido: "Então, em primeiro lugar, temos sido muito transparentes. **E a inteligência que estamos compartilhando é confirmada também com fontes abertas, com imagens de satélites comerciais.** Então, acho muito difícil contestar que a Rússia acumulou bem mais de 100.000 soldados e muito equipamento pesado." (tradução nossa, grifo nosso)
[37] Disponível em https://eng.mil.ru/en/news_page/country/more.htm?id=12409374
[38] Disponível em https://eng.mil.ru/en/news_page/country/more.htm?id=12409465
[39] Disponível em https://eng.mil.ru/en/news_page/country/more.htm?id=12409527

unidades na península da Crimeia.[40] Em posicionamento oficial, o porta-voz russo afirmou que se tratavam de movimentações relacionadas ao final do exercício conjunto com Belarus. A diplomacia russa também trabalhou para minimizar a escala da mobilização militar, afirmando que o medo de uma invasão da Ucrânia seria mera "histeria" do ocidente[41]. O porta-voz do Kremlin chegou a declarar que dita histeria ainda estaria longe de seu ponto culminante, e criticou as previsões da mídia ocidental acerca de uma invasão iminente. Vladimir Chizhov, embaixador russo para a União Europeia, em resposta às previsões diárias quanto ao início de um conflito armado, disse jocosamente que "as guerras na Europa raramente começam às quartas-feiras"[42].

Enquanto Rússia e os países do ocidente trocavam as acusações mencionadas, a opinião pública internacional pôde contar com uma terceira voz para compreender os eventos que se desenrolavam. Assim, comunidades online e indivíduos passaram a coletar e analisar dados de Fontes Abertas acerca da concentração militar russa, com a finalidade de validar ou refutar as narrativas estatais apresentadas.

3 . 3. 2 Verificação dos fatos utilizando OSINT

Nessa parte do presente trabalho, serão apresentados os relatórios publicados pelo Centre for Information Resilience (CIR). Trata-se de uma organização sem fins lucrativos baseada no Reino Unido, que tem por objetivo identificar e verificar InfOps perpetrados pelo que a própria organização chama de "atores hostis". Segundo a página da organização no LinkedIn[43], tais InfOps constituem ameaças à democracia e à verdade objetiva. Uma interessante iniciativa do CIR é o projeto "Eyes on Russia", iniciado em fevereiro de 2022, que documenta incidentes do conflito utilizando Fontes Abertas[44]. O projeto publica relatórios semanais, além de colaborar com outras organizações e indivíduos da comunidade OSINT na alimentação do *Russia-Ukraine Monitor Map*, um mapa colaborativo de incidentes verificados[45]. Segundo o próprio CIR, o banco de dados construído pela organização é utilizado pela mídia na cobertura dos acontecimentos na Ucrânia, por grupos que atuam na proteção de

[40] Disponível em https://eng.mil.ru/en/news_page/country/more.htm?id=12409336
[41] Disponível em https://www.bbc.com/news/av/world-europe-60411203
[42] Disponível em https://apnews.com/article/russia-ukraine-europe-russia-vladimir-putin-moscow-c7077c51178b52a32b0bb8740dffc1c1
[43] Disponível em https://apnews.com/article/russia-ukraine-europe-russia-vladimir-putin-moscow-c7077c51178b52a32b0bb8740dffc1c1
[44] O processo para a coleta e verificação dos dados pode ser consultado em https://www.info-res.org/post/eyes-on-russia-documenting-conflict-and-disinformation-in-the-kremlin-s-war-on-ukraine
[45] Disponível em https://maphub.net/Cen4infoRes/russian-ukraine-monitor

refugiados ucranianos, e por organizações focadas na responsabilização de violações de Direitos Humanos.

Tal qual a consideração feita sobre a Bellingcat, cabe esclarecer que o presente estudo não ignora o viés pró-Ocidente dos relatórios elaborados pelo CIR. Mantendo em mente que as análises elaboradas por esse ator podem não englobar pontos de vista contrários aos seus próprios interesses, espera-se que, ainda assim, seja viável levantar os subsídios necessários para responder à pergunta de pesquisa e testar a hipótese proposta.

A escolha do CIR para o presente estudo de caso se deve à colaboração de diversos atores, como a própria Bellingcat e outros, no mapa colaborativo de incidentes, bem como às datas de publicação dos primeiros relatórios, em janeiro e fevereiro de 2022. Espera-se que isso permita assimilar a evolução do conhecimento situacional da comunidade OSINT ao longo desse período. A utilização do *Russia-Ukraine Monitor Map* permitirá, também, exemplificar o tipo de informação que estava disponível publicamente na internet, à época dos fatos. Publicações de caráter jornalístico serão utilizadas de forma complementar, bem como declarações oficiais dos países envolvidos e respectivas autoridades.

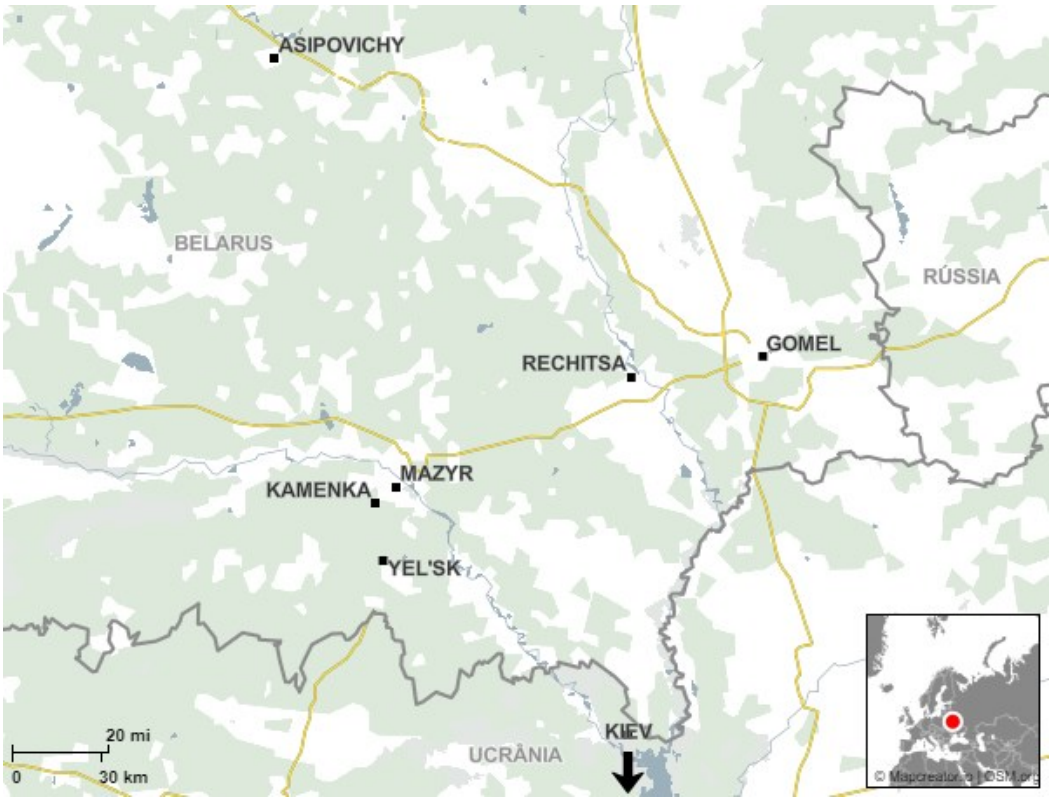
Os relatórios do CIR analisados englobam o período de 17 de janeiro a 22 de fevereiro de 2022, e correspondem aos 3 primeiros relatórios publicados. As datas de publicação são, respectivamente, 9 de fevereiro[46], 15 de fevereiro[47] e 22 de fevereiro[48]. O presente trabalho irá se debruçar, principalmente, sobre a seção "Military Movements" de cada um desses relatórios. Essa seção exibe apenas os eventos de acumulação e de movimentação de tropas que puderam ser verificados utilizando OSINT. As evidências de tais eventos, coletadas pelo CIR, foram registradas no *Russia-Ukraine Monitor Map*, o que permite que sejam apresentadas capturas de tela dos vídeos e de imagens satelitais utilizados. Para tal, aplicou-se no mapa os filtros "Russian Military Movements January 2022" e "Russian Military Movements February 2022", analisando as fontes coletadas de acordo com a data de publicação de cada relatório.

No primeiro relatório, os colaboradores do CIR conseguiram confirmar a localização de armamentos pesados sendo transferidos entre as cidades belarussas de Gomel, Rechitsa e Mazyr. Blindados foram detectados nas cidades de Kamenka e Yelsk. Sistemas lançadores de mísseis foram localizados na cidade de Asipovichy (CIR, 2022a, p.12). Destaca-se que essas cidades estão localizadas justamente na região mais próxima à Kiev, no "vazio geográfico"

[46] Disponível em https://www.info-res.org/post/launching-the-eyes-on-russia-project
[47] Disponível em https://www.info-res.org/post/eyes-on-russia-project-latest-developments
[48] Disponível em https://www.info-res.org/post/eyes-on-russia-report-3

onde não havia nenhuma base de operações prevista para o Union-Courage, conforme divulgação oficial do Ministério da Defesa russo.

Figura 7 - Locais de concentração de tropas e equipamentos militares russos em Belarus.



Fonte: elaborado pelo autor, com base em CIR (2022a)

Conforme mencionado, os registros citados pelo relatório do CIR estão mapeados no *Russia-Ukraine Monitor Map*. Abaixo são exibidas algumas capturas de tela do material coletado utilizando Fontes Abertas. Neste primeiro relatório, os dados analisados se referem principalmente aos últimos dias de janeiro de 2022. Embora a data das postagens ainda permita associar a concentração de tropas à preparação para o exercício conjunto com Belarus, o posicionamento de recursos militares em cidades que não constam na relação divulgada oficialmente já poderia levantar dúvidas acerca das reais intenções russas.

Tabela 3 - Monitoramento do transporte de blindados russos, utilizando Fontes Abertas.

Cidade	Plataforma	Data	Capturas de tela
Gomel	TikTok	24/01/2022	
Rechitsa	TikTok	25/01/2022	
Mazyr	TikTok	24/01/2022	

Fonte: elaboração própria, com base em CIR (2022a)

Figura 8 - Capturas de tela - Deslocamento de blindados russos em Kamenka, Belarus.

Plataforma: TikTok. Data: 24/01/2022. Fonte: Russia-Ukraine Monitor Map

Figura 9 - Sistema de mísseis russo Iskander, em Asipovichy, Belarus.
Plataformas e Datas: Twitter, 21/01/2022 (cima) e Maxar, 30/01/2022 (baixo).

Fonte: Russia-Ukraine Monitor Map

O primeiro relatório também aponta para movimentações de comboios em direção à península da Criméia. Conforme mencionado anteriormente, a região também era, no momento, palco de exercícios militares anunciados oficialmente pelo Kremlin. Vídeos postados em plataformas sociais, no final de janeiro de 2022, foram geolocalizados na cidade russa de Krasnodar, em direção ao Estreito de Kerch, e também já dentro da península. O monitoramento

dessa região é relevante tendo em vista que o governo russo também anunciou de forma oficial, em meados de fevereiro, a desmobilização dessas tropas.

Figura 10 - Imagens geolocalizadas.

Fonte: CIR (2022a) e Russia-Ukraine Monitor Map

Por fim, chama a atenção a ausência, nesse primeiro relatório, de menções às regiões do território russo próximas à fronteira com a Ucrânia. Os oblasts de Kursk, Belgorod e Rostov passam a receber maior atenção do CIR a partir do segundo relatório publicado. Em consulta ao *Russia-Ukraine Monitor Map* (ver figura 18), percebe-se o aumento substancial, ao longo do período estudado, de tropas localizadas por Fontes Abertas nessas três regiões russas.

O segundo relatório analisado utiliza materiais publicados no início de fevereiro de 2022. De acordo com o CIR (2022b, p.6), a acumulação de recursos militares russos na região sul de Belarus se manteve intensa na primeira quinzena de fevereiro. Esse segundo relatório traz novos comboios localizados nos oblasts russos de Kursk e de Belgorod, próximo à cidade ucraniana de Kharkiv. Equipamentos de comunicação militares, como um repetidor de rádio Rosoboronexport[49] R-419L1, foram instalados na cidade de Karaichnoe. Foram identificados,

[49] A Rosoboronexport é a única organização estatal na Rússia a exportar toda a gama de produtos, serviços e tecnologias militares e de uso dual. Fonte: http://roe.ru/eng/

também, ao menos seis comboios se movendo pelo oblast de Rostov, provavelmente em direção à Criméia (CIR, 2022b, p.6).

Figura 11 - Pontos de interesse no segundo relatório.

Fonte: CIR (2022b)

Figura 12 - Imagens geolocalizadas.

Fonte: CIR (2022b) e Russia-Ukraine Monitor Map

1: Rylsk, 09/02. 2: Korenevo, 11/02. 3: Veselaya Lopan, 08/02. 4: Karaichnoe, 08/02

Finalmente, será apresentado o terceiro relatório do CIR, que cobriu o período de 15 a 22 de fevereiro. Esse relatório foi o último publicado antes da invasão propriamente dita, e

apenas um dia após o governo russo reconhecer a independência das autoproclamadas repúblicas de Donetsk e de Lugansk[50]. No dia seguinte à publicação do relatório, o Kremlin informou que enviaria oficialmente tropas aos territórios separatistas[51]. Conforme mencionado anteriormente, a narrativa estatal russa já alegava, nesse período, que as forças militares participantes do Union-Courage e de outros exercícios estavam se desmobilizando e retornando às suas bases de origem. Contraditoriamente, o Ministro da Defesa de Belarus comunicou em 20 de fevereiro que os exercícios conjuntos seriam estendidos, devido ao "aumento da atividade militar perto das fronteiras da Rússia e da Bielorrússia, e a uma escalada da situação na região leste ucraniana de Donbas"[52].

As alegações de desmobilização das tropas também foram prontamente contraditas por meio de OSINT. "Equipamentos militares foram observados deixando bases maiores e espalhando-se para bases menores recém-criadas em campos ao longo da fronteira em Kursk e Belgorod." (CIR, 2022c, p.3, tradução nossa). Foram identificados equipamentos militares nas cidades belarussas de Naroulia e Kirov, a menos de 50km da fronteira com a Ucrânia, uma indicação de que os recursos militares russos estavam se aproximando da área de fronteira mais próxima à Kiev.

Ademais, tropas da Guarda Nacional russa (Rosgvardyia) foram geolocalizadas na cidade belarussa de Yelsk[53]. De acordo com o CIR (2022a, p.3), a Rosgvardyia funciona por fora da cadeia de comando normal, respondendo diretamente ao presidente Putin, o que seria um indicativo da prioridade atribuída pelo chefe de Estado às movimentações na região. No oblast russo de Belgorod, foram identificados, próximos à fronteira, blindados e outros veículos militares com a insígnia "Z" pintada na lataria[54]. Por fim, o relatório do CIR destaca o reagrupamento de tropas russas na cidade de Tomarovka, no oblast de Belgorod, com blindados sendo descarregados de trens.

[50] Disponível em http://en.kremlin.ru/events/president/news/67828
[51] Disponível em https://www.bbc.com/news/world-europe-60468237
[52] Disponível em https://www.reuters.com/world/europe/russia-belarus-extend-huge-military-exercises-belarus-ministry-2022-02-20/
[53] Os veículos foram identificados como pertencentes à Rosgvardyia pelas placas, como explicado em https://www.bellingcat.com/resources/how-tos/2022/02/08/tracking-russian-military-vehicles-on-the-move/
[54] A letra Z não consta no alfabeto cirílico, utilizado no idioma russo. Embora tenha sido inicialmente utilizada pelas forças russas como forma de identificação de suas próprias tropas, o símbolo passou a ser associado a manifestações pró-Rússia na internet, e foi incorporado à propaganda oficial do Kremlin. Fonte: https://www.bbc.com/news/world-europe-60644832

Figura 13 - Pontos de interesse no terceiro relatório.

Fonte: CIR (2022c)

Tabela 4 - Monitoramento do transporte de blindados russos, utilizando Fontes Abertas.

Cidade	Plataforma	Data	Capturas de tela
Naroulia	Twitter	18/02/2022	

Kirov	TikTok	18/02/2022	
Yelsk	Twitter	21/02/2022	
Skorodnoe	TikTok	22/02/2022	

Fonte: elaboração própria, com base em CIR (2022c)

Figura 14 - Comboio de blindados com a insígnia “Z”. Tomarovka, 22/02/2022.

Fonte: Russia-Ukraine Monitor Map

É possível observar, então, que os locais de identificação das tropas russas por Fontes Abertas se aproximam progressivamente da fronteira com a Ucrânia, no decorrer do período estudado. Uma análise dos registros efetuados no *Russia-Ukraine Monitor Map*, nos períodos relativos a cada um dos relatórios do CIR, corrobora esse aumento da atividade militar russa nas regiões fronteiriças. A figura 18 apresenta essa comparação:

Figura 15 - Evidências OSINT coletadas em Jan/21 (esquerda), entre 01/02 e 15/02 (centro), e entre 16/02 e 22/02 (direita).

Fonte: Russia-Ukraine Monitor Map

Ao se observar publicações na mídia tradicional nos dias imediatamente anteriores à invasão, constata-se que a consciência situacional da comunidade OSINT estava a par com aquela de atores com maiores recursos. Como visto anteriormente, o próprio CIR informa que o trabalho do grupo também é utilizado pela mídia tradicional na cobertura dos eventos em andamento. No entanto, quando grandes corporações como a BBC utilizam fontes comerciais em suas publicações, é evidente a similaridade com as fontes obtidas gratuitamente via plataformas sociais e publicizadas por cidadãos comuns.

A figura 19 ilustra o monitoramento, pela mídia tradicional, das posições russas no dia anterior à invasão. As fontes citadas pela BBC estão disponíveis comercialmente:

Figura 16 - Concentração de tropas russas próximo à fronteira com a Ucrânia.

Fonte: BCC[55]

Outra conclusão interessante que se pode inferir a partir das Fontes Abertas analisadas diz respeito às rotas iniciais da invasão propriamente dita. A despeito da negação oficial do Kremlin acerca de objetivos territoriais na Ucrânia[56], o monitoramento do avanço russo nos primeiros dias da invasão já indicava três possíveis alvos principais das forças russas: as cidades ucranianas de Mariupol e Kharkiv, e a capital Kiev.

Nesse contexto, percebe-se que as localidades onde os relatórios do CIR apontaram a presença militar russa coincidem com as linhas de frente após o início da invasão. Como mencionado, já no mês de janeiro as posições russas em Belarus poderiam lançar dúvidas sobre as reais intenções do governo de Putin (ver figura 10). As Fontes Abertas continuaram registrando a concentração de militares russos nessa região, e é plausível depreender que essas tropas avançaram em direção à Kiev após o anúncio da operação militar especial. Ademais, pode-se assumir que as tropas russas concentradas nas cidades de Ryl'sk e Korenevo avançaram em direção a Kiev, por vias ao norte da cidade ucraniana de Sumy. Mais ao sul, os militares

[55] Disponível em https://www.bbc.com/news/world-europe-60158694
[56] Disponível em http://en.kremlin.ru/events/president/transcripts/67843

concentrados na cidade de Veselaya Lopan teriam como objetivo inicial o assalto à estratégica cidade ucraniana de Kharkiv (ver figura 14). Por fim, as posições russas na Criméia e no oblast de Rostov, reveladas por meio da OSINT, teriam sido utilizadas para a entrada das forças russas nos territórios de Donetsk e Lugansk, e para o avanço sobre a cidade ucraniana de Mariupol. A figura 20, abaixo, exibe as linhas de avanço das forças russas efetivamente observadas nos primeiros dias da invasão militar.

Figura 17 - Avanço das tropas russas no início da invasão.

Fonte: BBC[57]

Em adição, são razoáveis certas inferências no tocante ao caráter exclusivamente defensivo dos exercícios militares, conforme alegado pelo governo russo. A mobilização de sistemas Iskander, citada nos relatórios do CIR, pode embasar argumentos para uma estratégia mais ofensiva, visto que esse armamento de mísseis guiados é capaz de empregar ogivas convencionais ou nucleares, e de atingir alvos a até 500km de distância[58]. Para efeito de comparação, uma estratégia puramente defensiva poderia ter se materializado na presença apenas do sistema antiaéreo S-400[59].

[57] Disponível em https://www.bbc.com/news/world-europe-60547807
[58] Disponível em https://www.military-today.com/missiles/iskander.htm
[59] Disponível em https://www.military-today.com/missiles/s400_triumph.htm

Um segundo indicativo de intenções ofensivas russas, citado nos relatórios, seria a mudança na organização geral das tropas russas. Conforme mencionado na apresentação do terceiro relatório, o CIR já havia identificado a desmobilização de grandes agrupamentos militares russos, que teriam sido, então, reorganizados em unidades táticas menores (CIR, 2022c, p.3). Enquanto uma formação em grande número pode ser entendida como uma demonstração de força militar, tais grupos não seriam acompanhados das linhas de suprimento necessárias para sustentar efetivamente um conflito[60]. Assim, a mudança para grupos menores e de maior mobilidade poderia sugerir preparações para ações iniciais de um conflito.

Finalmente, a instalação de hospitais de campanha e a mobilização de unidades aéreas. O CIR (2022b, p.7) menciona o estabelecimento de tais hospitais na primeira quinzena de fevereiro, embora não tenha sido possível localizar as evidências correspondentes no *Russia-Ukraine Monitor Map*. Por sua vez, o mapa registra um hospital instalado em 22 de fevereiro, conforme fonte reproduzida na figura 21, não mencionado pelos relatórios do CIR. A estrutura é identificada por sua cor distinta e pelo formato de cruz, como se pode ver na comparação da imagem. Não menos intrigante é a intensa mobilização de forças aéreas, como os helicópteros russos localizados por Fontes Abertas. Diversos vídeos publicados na internet permitem a identificação de unidades de helicópteros russos próximas à fronteira ucraniana, ao longo do mês de fevereiro. A figura 22 apresenta os dados registrados.

[60] Disponível em https://www.nytimes.com/2022/02/04/world/europe/russian-troops-ukraine-crimean-peninsula.html e https://www.nytimes.com/2022/02/21/world/europe/russia-military-ukraine-border.html

Figura 18 - Hospital de campanha geolocalizado em Belgorod (cima), em 22/fev. Hospital de campanha russo na Armênia, em 2020[61] (baixo).

Fonte: Russia-Ukraine Monitor Map.

[61] Disponível em https://armenpress.am/eng/news/1036240

Figura 19 - Helicópteros localizados via OSINT. (1) Belgorod, RUS, 12/fev. (2) Luje, BLR, 14/fev. (3) PushKarnoe, RUS, 17/fev. (4) Valuyki, RUS, 14/fev.

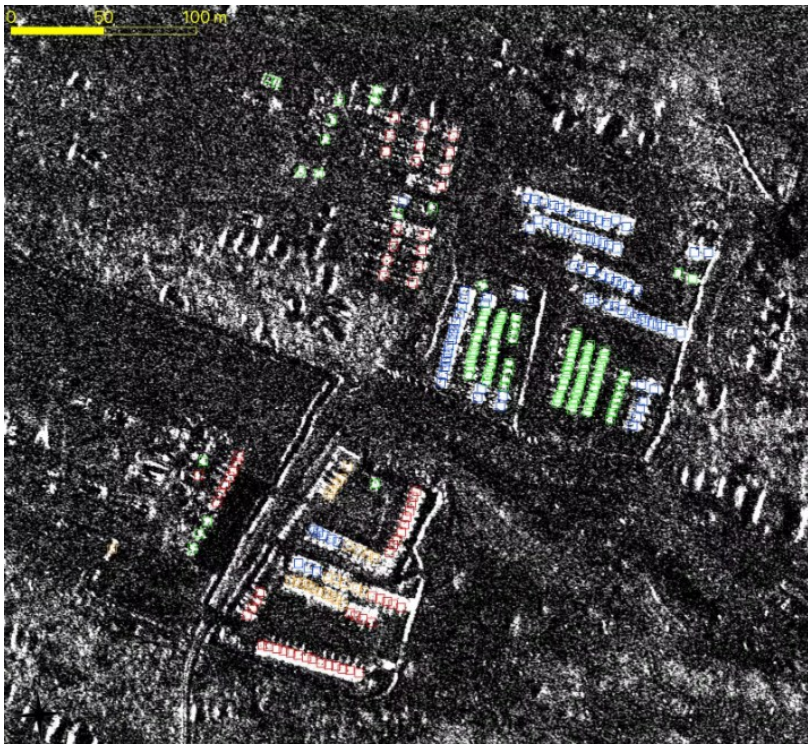
Fonte: Russia-Ukraine Monitor Map.

Isso posto, concede-se ser problemático afirmar que cada um desses indícios demonstra, por si sós, um caráter premeditadamente ofensivo dos exercícios militares, entretanto, a presença de todos em simultâneo ao longo da fronteira ucraniana por certo afasta a lógica de atividades militares meramente defensivas. Essa análise é complementada por informações divulgadas na mídia tradicional, como a estocagem de bolsas de sangue[62] e a quantidade recorde de tropas na região[63].

[62] Disponível em https://www.reuters.com/world/europe/exclusive-russia-moves-blood-supplies-near-ukraine-adding-us-concern-officials-2022-01-28/
[63] Disponível em https://www.vox.com/2022/2/18/22938886/russia-ukraine-crisis-troops-military-buildup

Uma outra análise a ser feita diz respeito ao uso da tecnologia de imagens de satélite por radar (SAR). Ao contrário do esperado inicialmente, nota-se mais uma vez a relativa ausência de imageamento por SAR no material analisado. Ao longo do desenvolvimento desta pesquisa, ficou evidente que a tecnologia SAR está disponível apenas comercialmente, via empresas privadas como Maxar, Planet e Capella Space. Algumas imagens SAR são divulgadas de forma gratuita por essas empresas, e têm sido então utilizadas pela comunidade OSINT, como apontado na figura 23. Deve-se considerar, naturalmente, o interesse de tais empresas na divulgação de imagens específicas. Em outros momentos, atores não estatais adquirem os produtos dessas empresas, pagando pelo acesso às imagens de radar e as utilizando em suas análises[64] (ver figura 24), o que não exclui a possibilidade de classificar esse material como proveniente de Fontes Abertas.

Figura 20 – Imagem SAR de baixa resolução, divulgada pela Capella Space em 06/jan, mostra um acampamento militar em Boyevo, Rússia.



Fonte: Asia Nikkei[65]

[64] Por exemplo, Bellingcat e Middlebury Institute of International Studies, citados no presente trabalho, possuem contratos de acesso a imagens de satélite especializadas. Fonte: https://www.bellingcat.com/resources/2021/09/21/bellingcat-can-now-access-specialised-satellite-imagery-tell-us-where-we-should-look/ e https://www.wired.com/story/ukraine-russia-satellites/

[65] Disponível em https://asia.nikkei.com/Politics/Ukraine-war/Ukraine-crisis-Satellite-imagery-reveals-growing-Russian-threat

Figura 21 – Imagem SAR obtida pelo Middlebury Institute of International Studies. O pesquisador Jeffrey Lewis menciona a capacidade da tecnologia SAR em capturar imagens em condições climáticas adversas.

Fonte: Twitter[66]

[66] Disponível em https://twitter.com/armscontrolwonk/status/1495941582436323330

3 Conclusões parciais

Na manhã do dia 24 de fevereiro, o governo russo abandonou por completo a retórica não intervencionista, anunciando formalmente uma "operação militar especial" na Ucrânia[67]. Segundo a inteligência estadunidense, o presidente Putin já havia decidido por uma invasão à Ucrânia no início de fevereiro, enquanto ainda negava publicamente que o faria[68], embora o Kremlin ainda estivesse considerando outras opções nos dois meses anteriores[69]. Conforme já apontado anteriormente neste capítulo, ambas as partes buscaram construir suas próprias narrativas acerca dos eventos em andamento, visando dominar o ambiente informacional e influenciar a opinião pública nos níveis nacional e internacional.

Nesse cenário, não se pode ignorar o papel exercido pela verificação, por terceiras partes e por fontes independentes, dos fatos e das narrativas envolvidos no conflito. Ao se estudar as ações de atores não estatais na esfera cibernética e informacional, fica evidente que estes dispõem de capacidades que até recentemente podiam ser consideradas exclusivas do Estado. Como no caso estudado, imagens de satélite e coordenadas de geolocalização estão hoje amplamente disponíveis na internet, permitindo que indivíduos e grupos atestem por si mesmos a veracidade de certas alegações estatais. Se houve um embate de narrativas em 2014 e 2015, entre Rússia e Ucrânia / EUA, acerca da participação militar russa no conflito no Donbas, indivíduos puderam coletar imagens de satélite, tanto comerciais quanto gratuitas, bem como fotos e vídeos publicados em redes sociais, para buscar, de forma independente, entender os fatos em andamento.

Assim como ocorreu na anexação da Criméia, em 2014, as narrativas estatais acerca dos eventos em andamento na Ucrânia, em 2022, puderam ser validadas ou refutadas por atores não estatais. No caso estudado, ficou evidente de que maneiras as movimentações das forças russas foram acompanhadas, de forma tempestiva e precisa, por organizações como CIR e Bellingcat. Ao passo em que o Kremlin afirmava que suas tropas estavam se retirando das áreas fronteiriças, a internet propiciou um ambiente para o compartilhamento de evidências, em sentido contrário, por parte de pessoas comuns, civis que estavam vivenciando os fatos em

[67] Disponível em http://en.kremlin.ru/events/president/news/67843
[68] Disponível em https://www.bbc.com/news/world-europe-60436938
[69] Disponível em https://theintercept.com/2022/03/11/russia-putin-ukraine-invasion-us-intelligence/. Destaca-se a estratégia heterodoxa de Biden ao publicizar dados de inteligência do governo dos EUA. "Com poucas outras opções disponíveis no último minuto para tentar deter Putin, o presidente Joe Biden deu o passo incomum de tornar a inteligência pública, no que se equivale a uma forma de guerra informacional contra o líder russo. [...] O uso antecipado da inteligência por Biden revelou 'um novo entendimento… de que o espaço da informação pode estar entre os terrenos mais importantes que Putin está contestando'" (tradução nossa).

primeira mão. Tais evidências foram disponibilizadas online sem nenhuma restrição de acesso, constituindo valiosas fontes primárias para analistas, jornalistas e pesquisadores.

Em contrapartida, provou-se um desafio a identificação, de forma objetiva, de qualquer reação oficial da Rússia à verificação de fatos e de narrativas pela comunidade OSINT. Notícias e declarações publicadas nos sites oficiais da Presidência e do Ministério da Defesa russos, entre 01 e 23 de fevereiro, não fazem menção à Fontes Abertas ou a atores não estatais. É factível que outras fontes oficiais que ficaram fora do escopo deste trabalho, como contas oficiais do governo e de autoridades russas no Twitter, possam fornecer elementos adicionais para a análise da reação do Estado russo às atividades desses atores não estatais. Redes de notícias estatais, como RT News e Sputnik, também podem fornecer um parâmetro para a visão oficial da Rússia no tocante às Fontes Abertas.

Dentro do escopo da concentração de tropas russas às vésperas da invasão, arrisca-se elencar algumas tomadas de decisão por parte do Kremlin durante o período analisado, e relacioná-las tentativamente à pressão internacional exercida pela comunidade OSINT. Por exemplo, tendo em vista que as alegações de desmobilização das tropas restaram enfraquecidas frente às evidências de Fontes Abertas em sentido contrário, chama a atenção a opção pela continuidade da presença militar no território de Belarus, mesmo após a data prevista para o encerramento do exercício conjunto.

A justificativa oficial passou a ser, então, o aumento das tensões no Donbas, causado pela "histeria do ocidente", e o envio de armamento pesado aos militares ucranianos[70]. Também foram feitas alegações de que a Ucrânia não estaria cumprindo os Acordos de Minsk, o que justificaria a manutenção das atividades militares na região[71]. É crível que a mudança de narrativa tenha sido uma adaptação das autoridades russas, uma vez que a simples negação reiterada da possibilidade de invasão não estava mais surtindo os resultados esperados sobre a agenda internacional.

Este capítulo teve como objetivo analisar um caso concreto que exemplificasse o exercício do poder da informação por parte de atores não estatais. A escolha pelo conflito entre Rússia e Ucrânia levou em conta a relevância do ambiente informacional e da dimensão cibernética, bem como a já reconhecida atuação da Comunidade OSINT nos eventos relacionados. A despeito da baixa disponibilidade de posicionamentos governamentais sobre as evidências de Fontes Abertas, objetivou-se demonstrar como tais fontes viabilizaram o

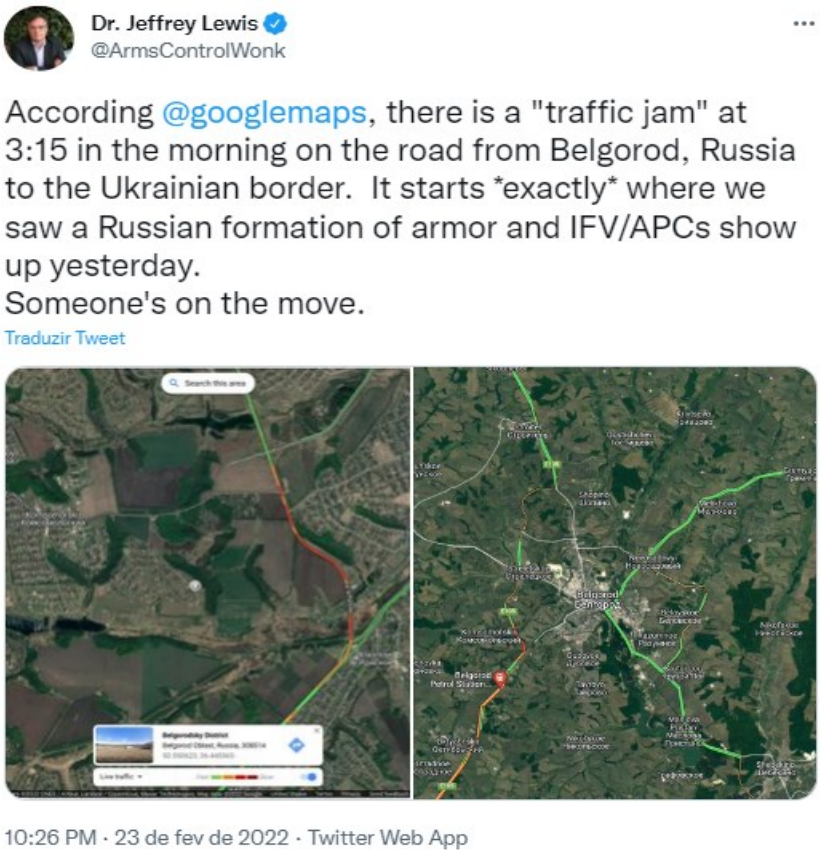
[70] Disponível em http://en.kremlin.ru/events/president/news/67759, http://en.kremlin.ru/events/president/news/67818 e http://en.kremlin.ru/events/president/news/67805
[71] Disponível em http://en.kremlin.ru/events/president/news/67809

exercício de poder por parte de atores não estatais. Por fim, também foi possível confirmar uma tendência de aumento desse aspecto do poder internacional, algo que indubitavelmente está, desde então, sendo considerado na tomada de decisão dos atores envolvidos.

4 CONSIDERAÇÕES FINAIS E PERSPECTIVAS FUTURAS

Someone's on the move. Às 3:15h da madrugada do dia 24 de fevereiro, horário local, pesquisadores do Instituto de Estudos Internacionais de Middlebury identificaram um engarrafamento na rodovia que liga Belgorod à fronteira com a Ucrânia[72]. A região estava sendo monitorada pelo grupo de pesquisa devido a imagens SAR obtidas dois dias antes, que mostravam uma unidade de tanques e veículos russos recém chegados e alinhados em colunas, prontas para deslocamento. A informação foi publicada no Twitter horas antes do discurso de Putin anunciando oficialmente a operação militar especial:

Figura 25 - Acompanhamento em tempo real da invasão da Ucrânia.

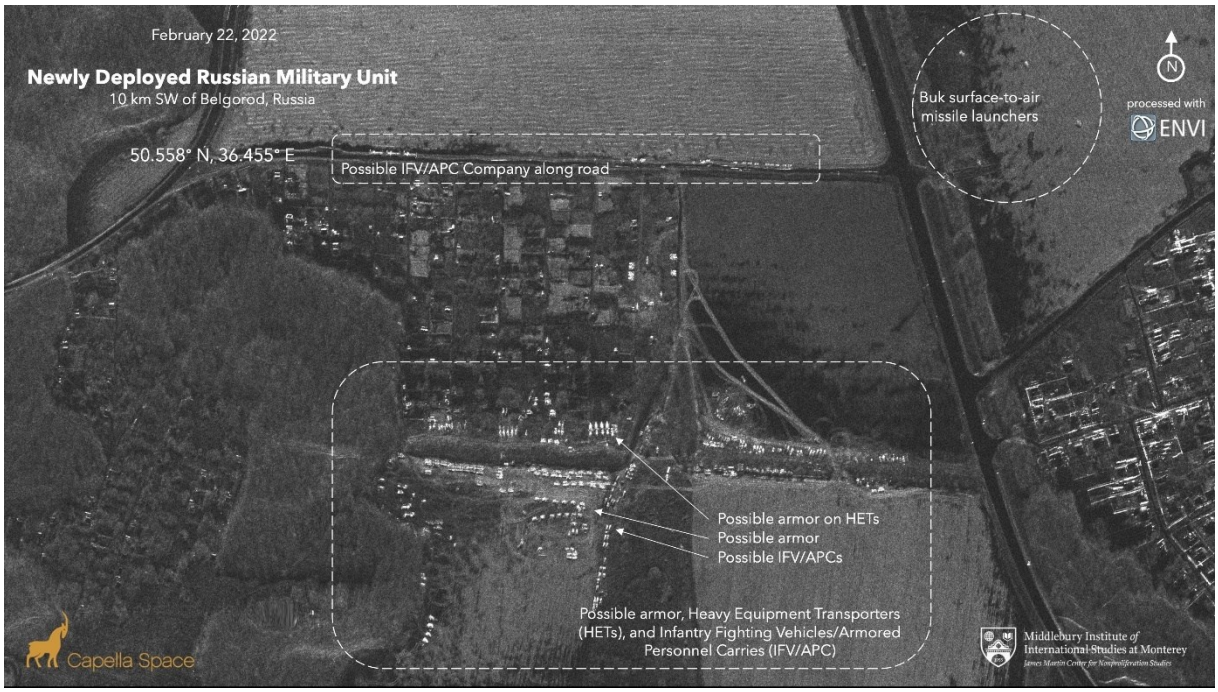


Fonte: Twitter[73]

Segundo o professor chefe da equipe de pesquisa, Dr. Jeffrey Lewis, o engarrafamento provavelmente foi registrado no Google Maps devido a veículos civis que estavam utilizando o aplicativo de navegação e foram impedidos de trafegar por causa do deslocamento militar. O pesquisador destaca, na imagem, a ausência de instalações como tendas ou alojamentos, o que indicaria o estado de prontidão daquela unidade[74].

[72] Disponível em https://www.middlebury.edu/institute/news/google-maps-tracking-invasion-ukraine
[73] Disponível em https://twitter.com/armscontrolwonk/status/1495941582436323330
[74] Disponível em https://www.wired.com/story/ukraine-russia-satellites/

Figura 26 - Imagem SAR.



Fonte: Twitter[75]

Desde então, o teatro de operações seguiu sendo acompanhado de perto pela comunidade OSINT. Diversos eventos ao longo do conflito, que ainda estava em andamento até o momento da conclusão deste trabalho, foram verificados utilizando Fontes Abertas. Apenas a título de exemplo, pode-se citar o uso de munições do tipo cluster[76], os ataques a alvos civis[77], e as denúncias de um massacre de civis na cidade de Bucha[78].

O contexto no qual os atores internacionais estão inseridos atualmente possui novidades significativas, em especial no que tange ao ambiente informacional e ao ciberespaço. Se o poder depende do contexto, então essa nova conjuntura implica em novas relações de poder entre os atores, e em uma nova distribuição de poder no sistema internacional. Ao longo deste trabalho, foi possível esmiuçar o aspecto informacional do poder internacional, ampliado pela expansão da cibernética, destrinchando-o em suas diversas manifestações. Para além da informação como instrumento de poder estatal, a literatura explorada viabilizou também o entendimento de sua função na própria estrutura do sistema internacional. A informação, assim, é empregada pelas unidades para moldar a estrutura a seu favor, ao passo em que tais mudanças sistêmicas também moldam o comportamento das próprias unidades.

---

[75] Disponível em https://twitter.com/ArmsControlWonk/status/1496668713373687808/photo/1
[76] Disponível em https://www.bellingcat.com/news/rest-of-world/2022/03/11/these-are-the-cluster-munitions-documented-by-ukrainian-civilians/
[77] Disponível em https://www.bellingcat.com/news/2022/03/17/hospitals-bombed-and-apartments-destroyed-mapping-incidents-of-civilian-harm-in-ukraine/
[78] Disponível em https://www.bellingcat.com/news/2022/04/04/russias-bucha-facts-versus-the-evidence/

Não menos importante, autores como Nye (2011) e Bramam (2006 apud Ávila e Pinheiro, 2014) expandem o quadro de análise ao apresentar uma interface entre as Relações Internacionais e outras áreas do conhecimento, como Ciência Política, Ciência da Informação e Sociologia. Essa perspectiva interdisciplinar possibilita o estudo do poder em seu aspecto comportamental, e um melhor entendimento de como os agentes se valem de diferentes faces do poder, a depender do contexto e dos objetivos almejados. Por essa linha de pensamento, a informação também é utilizada pelos atores de forma cooptativa, aspirando consolidar uma agenda internacional favorável a seus interesses, ou visando estabelecer as preferências iniciais dos demais participantes das relações de poder.

Pode-se dizer que a ampliação do quadro teórico foi uma resposta a mudanças expressivas nas relações internacionais e na sociedade como um todo. O início do século XXI testemunhou o crescimento exponencial da internet e a consolidação do espaço cibernético como domínio de projeção de poder. Como consequência dessa Revolução Digital, a dimensão cyber passou a dominar o Ambiente Informacional, que, por sua vez, se tornou ainda mais importante nas considerações sobre as capacidades dos atores internacionais.

Essas mudanças têm beneficiado principalmente aqueles atores considerados menores, que perceberam suas capacidades fortemente incrementadas. Observa-se uma redução da assimetria de capacidades entre atores estatais e não estatais, consequência de uma difusão de certos aspectos do poder internacional, propiciada pelas características intrínsecas ao ciberespaço e ao ambiente informacional. Conforme apontado por Nye (2011), difusão não é sinônimo de equalização de poder, mas implica em uma política internacional mais complexa e menos dominada pelos atores tradicionais. A Inteligência de Fontes Abertas é, assim, mais uma ferramenta por meio da qual indivíduos e grupos de indivíduos buscam executar suas estratégias de conversão de poder, visando influenciar o comportamento dos demais atores e atingir os seus resultados preferíveis.

É oportuno, então, retomar a hipótese que sustenta este trabalho. Buscou-se argumentos e exemplos para demonstrar que a difusão de poder, acelerada pela emergência do ciberespaço e de ferramentas como a OSINT, potencializa a ação de atores não-estatais em contextos de conflitos entre Estados. Foi possível depreender que o poder da informação constitui parte importante da capacidade dos atores internacionais, e que tal importância aumentou com a emergência e a consolidação do espaço cibernético. Ficou exemplificado, também, que persiste a tendência de aceleração dessa difusão, com esses atores obtendo cada vez mais facilmente acesso a tecnologias de ponta e a informações estratégicas. Por meio do estudo da Inteligência

de Fontes Abertas e de sua aplicação no conflito entre Rússia e Ucrânia, é plausível afirmar que o presente trabalho logrou ilustrar o mencionado aumento de poder de atores não estatais.

Em primeiro lugar, a comparação entre os eventos de 2014 e de 2022 permite inferir que, em um espaço de tempo consideravelmente curto, houve um aumento na quantidade e na qualidade da informação disponível a atores não estatais. No que tange à quantidade, a disseminação de dispositivos móveis e a popularização de plataformas sociais baseadas em vídeo viabilizou uma cobertura quase em tempo real do transporte de blindados e de armamento pesado por áreas rurais de um país em desenvolvimento. Em conflitos internacionais anteriores, esse tipo de informação teria sido censurado com relativa facilidade nos meios de comunicação tradicionais, devido ao seu caráter flagrantemente sensível para a estratégia de defesa e para o interesse nacional das partes envolvidas.

No que diz respeito à qualidade dos dados, é razoável mencionar o aumento na resolução dos vídeos e das imagens capturados por smartphones e outros dispositivos móveis, que facilita geolocalização das publicações via identificação de marcos geográficos e urbanísticos, placas veiculares e de trânsito, entre outros. Novas tecnologias, como o imageamento SAR, também aparentemente se tornaram mais acessíveis à comunidade OSINT nesses 5 a 7 anos que separam os eventos analisados[79], viabilizando a análise de imagens coletadas independentemente de condições climáticas adversas. Mesmo a disposição de veículos e de tendas em um acampamento militar, mais facilmente distinguível em imagens de satélite de alta resolução, leva os analistas a identificar quando se trata de um hospital de campanha, ou a depreender o estado de prontidão daquela unidade.

Em segundo lugar, é aceitável arrazoar que essa maior disponibilidade de informação tem resultado em um aumento na capacidade desses atores não estatais, uma difusão dos poderes cibernético e informacional, potencializando suas ações no cenário dos eventos de 2022. Conforme visto anteriormente, a informação pode ser fonte de poder internacional de diferentes maneiras: informação como um recurso a ser adquirido e negado aos opositores, dentro de um paradigma reducionista; informação como ferramenta a ser utilizada em uma relação de poder, visando obter o resultado desejado ao longo das três faces do poder comportamental; e informação como condicionante da própria estrutura internacional na qual os atores interagem, mensuram a diferença entre suas capacidades, e definem suas expectativas.

[79] A Bellingcat divulgou recentemente uma ferramenta que permite localizar sistemas de mísseis militares ativos, por meio da interferência que tais sistemas geram nas imagens de satélites SAR. Mais informações em https://www.bellingcat.com/resources/2022/02/11/radar-interference-tracker-a-new-open-source-tool-to-locate-active-military-radar-systems/

O estudo de caso apresentado exemplifica ao menos essa segunda forma de poder. Assim, no que tange às relações de poder, a capacidade informacional atual permitiu que atores não estatais, como a Bellingcat e o CIR, contrapusessem a narrativa apresentada pelo governo russo, refutando posicionamentos oficiais e, efetivamente, limitando a capacidade do Kremlin de consolidar uma agenda mais favorável frente à opinião pública internacional. Em outros termos, esses atores considerados menores adquiriram e ampliaram sua capacidade de exercer *Soft Power* dentro da segunda face do poder relacional, moldando em certa medida a agenda internacional. Esses atores não foram capazes de sobrepujar a vontade da Rússia, impedindo, por exemplo, que a invasão ocorresse. Difusão de poder não significa equalização de poder (Nye, 2011, p.132). Entretanto, tais atores conseguiram tornar a opinião pública mais resistente à cooptação pela narrativa russa, reduzindo a legitimidade desta, e provavelmente influenciaram a racionalidade do Kremlin a respeito de suas opções viáveis:

> A disseminação da informação significa que o poder será mais amplamente distribuído, e as redes informais irão minar o monopólio da burocracia tradicional. A velocidade da Internet significa que todos os governos têm menos controle de suas agendas. Os líderes políticos desfrutarão de um menor grau de liberdade antes de precisarem responder aos eventos e, então, terão que dividir o palco com mais atores. (NYE, 2011, p.116)

Por essa linha de pensamento, e considerando as decisões tomadas pelo governo russo, faz sentido aduzir que este viu diminuídas as suas opções de *Soft Power* enquanto mobilizava suas forças armadas para posições estratégicas. Consequentemente, o governo russo poder ter se tornado mais inclinado a se valer de instrumentos coercitivos, mesmo em situações onde a cooptação teria sido mais eficaz e menos desgastante politicamente.

Por outro lado, é interessante tecer considerações sobre certos elementos, identificados ao longo desta pesquisa, que mereceriam um maior aprofundamento, obstado pelos limites de tempo e de escopo da mesma.

Primeiramente, grande parte da argumentação apresentada se baseia na premissa de que a Era da Informação tem o efeito de dissipar a névoa da guerra, isto é, de reduzir as incertezas a respeito dos eventos em andamento durante um conflito internacional. Mas o imenso volume de informações gerado pela expansão do ciberespaço pode, também, ter justamente o efeito oposto, dificultando com que se filtre os ruídos e se obtenha os dados relevantes a tempo de ainda constituírem uma vantagem estratégica para o tomador de decisão. Técnicas como a Mineração de Dados e ferramentas como a Inteligência Artificial podem ser parte da solução pra que os atores administrem essa sobrecarga informacional. Além disso, convém mencionar que a Inteligência de Fontes Abertas também apresenta vulnerabilidades passíveis de serem exploradas pelas partes de um conflito. A disseminação massiva das chamadas *Fake News* e o

uso de *Deep Fakes*[80] pode tornar impraticável o trabalho de verificação de fatos, exaurindo os recursos desses agentes não estatais. A questão da audiência alvo também é importante, e cabe questionar se a censura estatal dos meios de comunicação, incluindo as redes sociais e serviços de mensagem instantânea[81], é o suficiente para impedir que a opinião pública de determinado país tenha acesso ao conhecimento obtido por meio da OSINT.

Outro apontamento pertinente se refere a algumas das fontes primárias utilizadas neste trabalho. Como se pôde perceber na apresentação das organizações Bellincat e Centre for Information Resilience (CIR), ambas possuem um forte viés pró-ocidente. Ainda que os vídeos e imagens de satélite coletados por essas organizações estejam disponíveis também ao público em geral, para verificação das análises desses atores, é razoável afirmar que as tais análises contam apenas parte da história do conflito. Nota-se, por exemplo, que os relatórios estudados não informam em nenhum momento a posição das forças ucranianas, uma informação sensível e que poderia ser utilizada contra os interesses de Kiev. Um estudo mais aprofundado sobre como atores pró-Rússia utilizam OSINT a seu favor poderia evidenciar novos atributos dessa guerra informacional moderna.

Adicionalmente, à medida que a Inteligência de Fontes Abertas ganha destaque e reconhecimento pelos resultados alcançados, pode-se levantar hipóteses acerca dos seus limites atuais e futuros. Plataformas utilizadas na coleta de dados abertos, como Google Earth e Google Maps, são fornecidas por empresas privadas, que podem optar por restringir o acesso público de informações concernentes a regiões de conflito. Empresas comerciais de imagens de satélite, como Maxar e Cappela Space, largamente utilizadas pela comunidade OSINT, são sediadas nos EUA e possuem contratos de defesa com o governo estadunidense[82]. Pode-se questionar se tais empresas são seletivas com os clientes que adquirem seus produtos, ou mesmo com os usuários cujo acesso é concedido gratuitamente para fins acadêmicos.

Por fim, a popularidade e a efetividade da OSINT em zonas de conflito podem mesmo encorajar controles estatais mais rígidos sobre o acesso a certas tecnologias, o que acarretaria em uma reversão da tendência de aumento na disponibilidade de informação a atores não estatais. Não se pode esquecer, afinal, que também no espaço cibernético o Estado Nacional detém a *ultima ratio*.

---

[80] Disponível em https://www.bbc.com/portuguese/internacional-60791955
[81] Disponível em https://www.theguardian.com/world/2022/mar/04/russia-completely-blocks-access-to-facebook-and-twitter
[82] Disponível em https://www.cnbc.com/2022/05/25/nro-announces-satellite-imagery-contracts-to-maxar-planet-blacksky.html

REFERÊNCIAS

AFONSO, Leonardo Singer. **Fontes abertas e Inteligência de Estado**. Revista Brasileira de Inteligência, v. 2, n. 2, p. 49-62, 2006.

ALBERTS, David S. et al. **Understanding information age warfare.** Assistant secretary of defense (C3I/Command Control Research Program), Washington DC, 2001.

ARQUILLA, John; RONFELDT, David. **Cyberwar is coming! Comparative Strategy**. v. 12, n. 2, p. 141-165, 1993.

ÁVILA, Rafael Oliveira de; PINHEIRO, Marta Kerr. **Poder Informacional nas Relações Internacionais Contemporâneas**. Monções: Revista de Relações Internacionais da UFGD, v. 3, n. 5, p. 23-52, 2014.

BELLINGCAT. Russia's Path to War: **A Bellincat Investigation**. 2015.

BLANK, Stephen. **Cyber war and information war a la russe. Understanding cyber conflict: Fourteen analogies**, p. 1-18, 2017.

CARAFANO, James Jay. **America's Joint Force and the Domains of Warfare**. Heritage, October, v. 4, 2017.

CARR, Edward Hallett. **Vinte anos de crise: 1919-1939**. ED. Universidade de Brasília, 1981.

CASTELLS, Manuel. **The rise of the network society**. Oxford, 2010.

CEPIK, Marco. **Espionagem e democracia**. FGV Editora, 2003.

CIR. Eyes on Russia Project. Report 1. 2022a. Disponível em <https://www.info-res.org/post/launching-the-eyes-on-russia-project>. Acessado em 28/07/2022.

CIR. Eyes on Russia Project. Report 2. 2022b. Disponível em < https://www.info-res.org/post/eyes-on-russia-project-latest-developments>. Acessado em 28/07/2022.

CIR. Eyes on Russia Project. Report 3. 2022c. Disponível em <https://www.infores.org/post/eyes-on-russia-report-3>. Acessado em 28/07/2022.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra cibernética: a próxima ameaça à segurança e o que fazer a respeito.** Brasport, 2015.

CONNELL, Michael; VOGLER, Sarah. **Russia's approach to cyber warfare**. Center for Naval Analyses, Arlington, United States, 2017.

Department of Defense https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf, 2014.

Department of Defense. Dictionary of Military and Associated Terms. Joint Publication 1-02. https://dcsg9.army.mil/assets/docs/dod-terms.pdf, 2007.

GIBSON, Stevyn. **Open source intelligence: An intelligence lifeline**. The RUSI Journal, v. 149, n. 1, p. 16-22, 2004.

KLANOVICZ, Jó. **Fontes abertas: Inteligência e o uso de imagens**. Revista brasileira de inteligência, v. 2, n. 2, p. 63-75, 2006.

KUEHL, Daniel T. **From cyberspace to cyberpower: Defining the problem. Cyberpower and national security**, v. 30, 2009.

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

MIELNICZUK, Fabiano. **Identidade como fonte de conflito: Ucrânia e Rússia no pós-URSS**. Contexto internacional, v. 28, p. 223-258, 2006.

MORGENTHAU, Hans Joachim. **Politics among nations: The struggle for power and peace**. 1985.

NYE, Joseph S. **The future of power**. Public Affairs, 1ª ed, 2011.

NYE, Joseph S. Soft Power: **the means to success in world politics**. New York: Public Affairs, 2004.

SINGER, P. W; FRIEDMAND, Allan. **Cybersecurity and cyberwar: what everyone needs to know**. Oxford, 2014.

SHVEDA, Yuriy; PARK, Joung Ho. **Ukraine's revolution of dignity: The dynamics of Euromaidan**. Journal of Eurasian Studies, v. 7, n. 1, p. 85-91, 2016.

TZU, Sun. **A arte da guerra**. Editora Schwarcz - Companhia das Letras, 2019.

UNVER, Akin. **Digital Open Source Intelligence and International Security: A Primer**. EDAM Research Reports, Cyber Governance and Digital Democracy, v. 8, 2018.

VENTRE, Daniel. **Cyberconflict: Stakes of Power**. In: Cyberwar and information warfare, John Wiley & Sons, 2012.

WALTZ, Kenneth N. **Realist thought and neorealist theory**. Journal of International Affairs, p. 21-37, 1990.

WALTZ, Kenneth. **Reductionist and systemic theories**. In: Neorealism and its Critics, p. 47-69, 1986.

WILLIAMS, Heather J.; BLUM, Ilana. **Defining second generation open source intelligence (OSINT) for the defense enterprise**. Rand Corporation, 2018.

Yin, R. K., & Campbell, D. T. (2018). **Case study research and applications : design and methods (Sixth edition.)**. Thousand Oaks, California: SAGE Publications, Inc.