AUSTRAL: Revista Brasileira de Estratégia e Relações Internacionais
e-ISSN 2238-6912 | v.14, n.27, Jan./Jun. 2025 | p.41-63

A DESINFORMAÇÃO NAS RELAÇÕES INTERNACIONAIS: EXAMINANDO AS VULNERABILIDADES DO BRASIL

Leandro Loureiro Costa[1]

Introdução

A expansão das Tecnologias de Informação e Comunicação (TICs), no início do século XXI, aumentou consideravelmente a importância do papel da internet na vida dos indivíduos. Embora não exista um conceito consensual para as TICs, elas geralmente são descritas como um conjunto abrangente de dispositivos, aplicações, componentes de rede, dados, sistemas e infraestruturas que estão envolvidas com a computação moderna. Desse modo, a internet, celulares, programas de computador, redes sociais, redes sem fio, e outros serviços que possibilitam o acesso, o armazenamento, a transmissão e o processamento de dados, são considerados tipos de TICs.

A evolução dos sistemas e ferramentas que circundam esse tipo de tecnologia e o aumento da conexão entre as sociedades também trouxeram novas ameaças. Nesse contexto, assuntos como segurança da informação, crimes cibernéticos, segurança e defesa do ciberespaço entraram na agenda de diversos Estados, sobretudo das Grande Potências.

O Brasil, pelo menos através de documentos normativos, tem dado relevância ao tema. As edições da Política Nacional de Defesa têm continuamente explicitado que o setor cibernético é estratégico para o país, enfatizando a necessidade de capacitar as tecnologias de informação e comunicação, não só as das Forças Armadas, mas também as de todas as estruturas do Estado. Além disso, através da Estratégia de Segurança Cibernética (E-Ciber 2020), o Brasil aponta que o recrudescimento do desenvolvimento da área de tecnologia da informação e comunicação causou um aumento no uso do ciberespaço para diversas atividades, inclusive na oferta de serviços públicos. Ademais, a expansão das TICs possibilitou um crescimento exponencial nas interações sociais na dimensão cibernética.

1 Universidade Federal do Rio de Janeiro, Rio de Janeiro, Brasil. E-mail: leandroloureirocosta@gmail.com. ORCID: https://orcid.org/0000-0003-3787-9015.

41

No âmbito das grandes potências, com a anexação da Crimeia pela Rússia e o apoio de Moscou a organizações separatistas no leste ucraniano, autoridades dos Estados Unidos têm registrado a expansão de campanhas de desinformação patrocinadas pelo Kremlin contra Washington e seus aliados. Esse avanço se dá a partir de veículos estatais de comunicação, como a Russia Today e o Sputnik, mas também através do aumento da presença em redes sociais com a contratação de trolls e a criação de novos emissores de informação (Bunce e Hozic 2016, 440).

Em 2017, alguns relatórios da inteligência estadunidense sugeriram a possibilidade do governo russo ter financiado a fabricação e a disseminação de desinformação durante as eleições presidenciais nos EUA para prejudicar a campanha da candidata do Partido Democrata, Hillary Clinton. Após esse evento, a União Europeia (UE) e a Organização do Tratado do Atlântico Norte (OTAN) patrocinaram a construção do Centro de Excelência de Comunicações para a Contenção de Ameaças Híbridas em Helsinque, com o intuito de investigar possíveis ameaças de emprego de desinformação em relação à Europa (Lanoszka 2019). Por outro lado, no mesmo ano, a Rússia também alertou sobre a possibilidade de campanhas de desinformação por parte da Europa e principalmente dos EUA, com acusações sobre Washington estar patrocinando campanhas de desestabilização em várias regiões do mundo, inclusive na Ucrânia, em 2014, durante o Euromaidan.

Cada vez mais, os Estados têm despendido investimentos em suas capacidades de disseminação de propaganda e desinformação em grande escala com o objetivo de alterar a forma como as pessoas pensam e também como elas agem. Não somente isso, cada vez mais os atores no sistema internacional têm investido em meios de proteção para combater esse tipo de ameaça, como por exemplo o banimento de portais da mídia estatal russa realizado por países componentes da UE e o Canadá ou o chamado Projeto Escudo Dourado da China, que bloqueia o conteúdo de diversos sites considerados como ameaças à segurança, tal como o Voice of America (Nichols e Corrêa 2023).

No bojo da segurança da informação, as revelações de Edward Snowden em 2013, sobre o programa de espionagem realizado pela National Security Agency dos EUA, expuseram que autoridades brasileiras, como a presidente Dilma Rousseff, tiveram seus telefones grampeados pela agência de inteligência estadunidense. Além disso, a Petrobras também havia sido espionada. Somado a esse caso, de acordo com a BNAmericas (2020) o Brasil é o segundo país mais afetado por crimes cibernéticos, totalizando 70 milhões de vítimas e produzindo 80 bilhões de dólares de perdas financeiras.

Desse modo, justifica-se a necessidade de se investir qualitativamente

e quantitativamente em pesquisas sobre os impactos dessa nova conjuntura no Brasil. O objetivo desta pesquisa é identificar as vulnerabilidades do país quanto aos impactos de operações de desinformação promovidas por atores estatais ou não-estatais. Traçar novas considerações sobre as fraquezas do Estado quanto a campanhas de desinformação também é uma contribuição para a análise do desenvolvimento tecnológico do país em um contexto de segurança nacional, principalmente no que tange o setor das TICs. Nesse caso, o setor cibernético deve ser percebido como parte indispensável da estratégia nacional.

Também é necessária a realização de pesquisas sobre as potencialidades e as vulnerabilidades do Brasil em um contexto de competição no sistema internacional, onde diversos atributos do setor das TICs podem causar impactos na distribuição de capacidades materiais entre Estados. Neste ensejo, tecnologias como a internet das coisas, inteligência artificial, 5G, realidade virtual e aumentada e big data adquirem importância estratégica. Tudo isso, somado à necessidade cada vez maior de microprocessadores e outros tipos de hardware, demanda que o Brasil, Estado que se propõe como potência, desenvolva as suas indústrias nos termos dessas novas tecnologias de modo a competir com os principais atores do sistema internacional, além de garantir a sua própria segurança.

Metodologia

Este estudo aborda o conceito de desinformação aplicando-o nas Relações Internacionais (RI). Neste processo, é detalhada a relação desse termo como parte da estratégia de subversão. Para isso, a literatura sobre esta terminologia é revista de forma a situá-la nas dinâmicas de competição existentes no sistema internacional. Desse modo, será discutida a análise de Lanoszka (2019) sobre a eficiência das operações de desinformação em alterar as políticas de um Estado.

São testadas no caso do Brasil, três hipóteses construídas por Lanoszka (2019) sobre a ineficácia das campanhas de desinformação quanto à produção de mudanças nos Estados-alvo de acordo com os interesses do perpetrador: H1) a anarquia internacional gera incertezas sobre quaisquer informações transmitidas pelos adversários, logo os governos rivais sempre irão esperar as piores ações dos inimigos e vão construir meios de proteção em relação a elas; H2) os cidadãos geralmente confiam mais nas suas experiências prévias, possuem pré-conceitos sobre as elites políticas estrangeiras e seriam mais propensos a adotarem perspectivas ideológicas quando pensam

sobre a dimensão internacional, do que as elites do Estado, fato que amplia a dificuldade de influência advinda de atores externos; H3) o Estado pode utilizar contramedidas mesmo em um cenário de polarização política, ele não é incapaz de tomar ações para reduzir os impactos das campanhas de desinformação e até mesmo desenvolver uma contra-campanha de desinformação para minimizar os danos da operação adversária.

Com a testagem das hipóteses é possível realizar um mapeamento do Brasil quanto às percepções sobre os riscos e políticas de defesa quanto à segurança da informação e segurança cibernética. Torna-se factível a elaboração de um exame sobre as ameaças potenciais ao país no campo da informação, a formulação de novas hipóteses para serem testadas em outras investigações, a criação de contribuições para teorizações futuras em torno do tema da subversão.

A metodologia adotada objetiva fornecer um entendimento concreto sobre o atual contexto, de forma a explorar as principais vulnerabilidades do Brasil quanto a campanhas de desinformação. Essa análise tem como objetivo contribuir para o planejamento de instituições civis e militares de forma a minimizar possíveis ocorrências e garantir vantagem competitiva ao país em eventos tangentes ao tema da instrumentalização da informação para a desestabilização política.

O conceito de ciberespaço

É importante ressaltar que, de acordo com Kramer et al. (2009), há mais de 28 definições sobre ciberespaço, o que revela uma falta de consenso conceitual. Porém, em um projeto capitaneado pela professora Nazli Choucri (2015) envolvendo uma série de instituições, denominado "Explorations in Cyber International Relations", considera-se o ciberespaço englobando I) estruturas físicas e dispositivos de telecomunicação que permitem a conexão de redes de sistemas tecnológicos e de comunicação; 2) sistemas de computador; 3) redes entre sistemas de computadores; 4) redes de redes que conectam sistemas de computadores; 5) os nós de acesso dos usuários e os nós intermediários de roteamento; 6) dados constituintes.

O ciberespaço é um domínio estratégico, porém também é um domínio social. Na Doutrina Militar de Defesa Cibernética (Ministério da Defesa 2023) do Brasil, o espaço cibernético é visto como uma dimensão virtual que é formada por dispositivos computacionais conectados a redes, em que informações digitais são transmitidas, processadas e armazenadas. Além disso, o espaço cibernético é classificado como uma área de atuação da defesa

cibernética, conceituada como um conjunto de práticas realizadas no contexto de um planejamento nacional de nível estratégico com o objetivo de "proteger os ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente". Já o Livro Branco de Defesa Nacional de 2020 (LBDN) considera o espaço cibernético como um cenário de ameaças de caráter multifacetado, tanto estatais, quanto não-estatais, que podem colocar em risco a integridade das infraestruturas críticas determinantes para os sistemas associados à segurança do país.

Daniel Ventre (2013) configura o ciberespaço como um domínio estratégico e social. O autor divide o espaço cibernético em três camadas. A primeira é a do hardware e corresponde a um conjunto de dispositivos físicos capazes de suportar a segunda camada, que é a camada virtual de programas, aplicativos e informações (software), que por sua vez são usados e manipulados pela camada cognitiva de usuários, chamada de "peopleware". A abordagem de Ventre suporta o conceito de que o ciberespaço é moldado pela experiência dos usuários. A existência da camada de peopleware socializa o ciberespaço, não o considerando apenas de um ponto de vista eletrônico e/ou mecânico. O uso que o peopleware faz do ciberespaço é o que o transforma em um espaço de relações sociais e, portanto, um espaço de poder.

Essa nova dimensão operacional é explorada substancialmente nas mídias sociais, onde o compartilhamento em massa de informações pessoais por parte dos usuários eleva os riscos para a segurança nacional. A flexibilidade da privacidade possibilita a personalização do conteúdo a partir do perfil do usuário, que é definido através da coleta de dados durante o acesso às plataformas, ou até quando elas não estão sendo utilizadas. Essa seleção é realizada por algoritmos e isso permite a disseminação de narrativas adaptadas ao gosto do usuário. Desse modo, há o recrudescimento da possibilidade de se afetar o campo cognitivo do indivíduo graças à facilidade de compartilhamento, à velocidade de alastramento e ao alcance do conteúdo publicado nas mídias sociais (Stassun e Assmann 2012; Nichols e Corrêa 2023).

A informação e a desinformação nas RI

O avanço de tecnologias de análise de dados, inteligência artificial e aprendizagem de máquina tem revolucionado tanto a capacidade de influenciar economicamente e politicamente outros atores, como a tomada de decisões em relação à segurança. Também tem possibilitado a utilização de informação

como forma de coerção e manipulação em grande escala e tem aumentado substancialmente a velocidade de comunicação. O grau de relevância desse processo pode ser observado na Estratégia Nacional dos Estados Unidos em 2017, que possui um capítulo sobre 'information statecraft', que também destaca os possíveis riscos advindos da Rússia e da China sobre esse tema (Rosenbach e Mansted 2019).

Os Estados têm realizado uma "corrida de soma-zero" pela extração de dados e sua operacionalização. É um setor que tende a ter empresas monopolistas devido a um ciclo virtuoso: quanto mais dados se obtém, mais as aplicações desenvolvidas por essas corporações são aprimoradas, esse processo aumenta os lucros e garantem ainda mais habilidades para extrair e instrumentalizar maiores quantidades de dados. Esse acúmulo de dados torna-se uma ferramenta relevante para o emprego da desinformação através da utilização dos algoritmos para direcionamento de conteúdo.

A desinformação é um tipo de informação que tem como objetivo produzir engano. Entende-se como campanha de desinformação a busca sistemática de um ator influenciar o processo político, através da utilização da desinformação para enganar uma audiência (Fallis 2011; Lanoszka 2019). A desinformação é um componente do processo das operações de deception, que buscam manipular as crenças para a obtenção de vantagens e produzir uma relação de coerção. Rid (2020) indica que em meados dos anos 2010, as operações de desinformação ganham um novo formato a partir de inovações tecnológicas e da cultura da internet. Nessa nova era, as campanhas são mais velozes, não demandam qualificação operacional e podem ser realizadas remotamente e de forma descentralizada.

Um fator complicador é o uso político que se faz do termo desinformação. Ao indicar que outro ator está praticando campanhas de desinformação, o acusador busca enfraquecer a confiança nas informação que são emitidas pelo alvo acusado, legitimar censuras e sanções e também fortalecer a própria legitimidade. As acusações mútuas por parte de Estados Unidos e Rússia são exemplos de utilização da terminologia "desinformação" com o intuito de tentar influenciar a opinião pública. Por exemplo, durante os conflitos na Ucrânia, a Casa Branca acusou Moscou de espalhar desinformação para justificar suas ações militares, com alegações de genocídio na região do Donbass ou a possibilidade de laboratórios de armas biológicas ucranianas. Os Estados Unidos também acusaram o Kremlin de patrocinar narrativas contra as vacinas fabricadas por empresas estadunidenses durante a pandemia da Covid-19. Por seu turno, a Rússia também acusou os Estados Unidos de usar desinformação para tentar desestabilizar os governos que não são alinhados com o Ocidente e para incitar protestos internos na Rússia.

Quanto à perspectiva teórica, o tema da desinformação é pouco debatido nas RI. O realismo estrutural privilegia o status da distribuição das capacidades materiais no sistema internacional e não há um consenso quanto ao tratamento da inteligência/contra-inteligência como uma capacidade material. Lanoszka (2019, 5) aponta que uma hipótese para corroborar o entendimento da inteligência como componente das capacidades materiais é a compreensão da inteligência como ferramenta capaz de empoderar um Estado em relação ao outro. Nesse caso, as campanhas internacionais de desinformação podem ser consideradas na lógica realista estrutural ao interpretá-las como um instrumento que possibilita minimizar as capacidades materiais do alvo ou enfraquecer o processo político da sociedade alvo.

Embora não tratassem diretamente da desinformação, os realistas clássicos consideravam o papel da informação, traduzido pelo fator cultural, que tem a capacidade de influenciar as formas pelas quais os Estados buscam aumentar o seu poder. Morgenthau destaca o 'imperialismo cultural' como aquele mais efetivo, que busca o controle das mentes dos indivíduos com o objetivo de alterar as relações de poder entre as nações Já Carr menciona o poder sobre a opinião, que é condicionado pelo status, pelo interesse e pela superioridade econômica e militar, que permitem facilmente impor estas ideias a outros. Enquanto isso, Aron aponta a "ideia" como um dos três objetivos perseguidos pelos Estados, ao lado da potência e da glória (Suppo 2011, 49).

Lanoszka (2019, 5) afirma que as teorias racionalistas são as melhores para acessar os efeitos da desinformação, devido ao fato de assumirem que a informação possui relevância nas relações internacionais. Rathbun (2007) afirma que os racionalistas concordam com os realistas estruturais que a anarquia gera incerteza quanto às intenções de outros atores, mas essa incerteza pode ser administrada. Glasser (1994) afirma que os Estados podem adquirir informações sobre as intenções dos outros Estados que poderiam classificá-los como defensores do status quo ou como atores revisionistas, ou entre Estados de característica ofensiva ou defensiva.

Para Lanoszka (2019, 6), não há motivos para indicar que a anarquia internacional tem menos força na relação entre Estados que praticam a desinformação e os que são alvos dessas campanhas. Ao contrário, a desinformação provoca a erosão da confiança e das normas e os inimigos são os principais alvos desse tipo de operação. Esse contexto é mais similar ao sistema anárquico internacional do que um sistema onde a anarquia é constrangida (Lanoszka 2019, 6).

De fato, a anarquia internacional parece ditar as dinâmicas existentes no processo de desinformação, pois as principais operações desse tipo

ocorreram em momentos onde ela se materializou explicitamente, e.g. as campanhas contra o Japão na década de 1920 propagadas por Moscou e as da CIA contra a Alemanha Oriental. Entretanto, é importante frisar que o antagonismo direto não precisa estar presente para a utilização de campanhas de desinformação e é preciso ter em conta que o ator que empreende a operação tem como objetivo alterar o comportamento do seu alvo para pender a balança de poder ou mantê-la ao seu favor, ou de desestabilizá-lo internamente.

O fato da anarquia internacional existir não imprime uma relação de causalidade na construção de "barreiras" e "filtros" que irão permitir que um Estado bloqueie todas as informações advindas de outros atores. No sistema internacional conflituoso, os Estados vão se esforçar para buscar novas áreas de influência e também manter as que já existem. O fato de encontrarem algum tipo de resistência não é um impedimento para que deixem de instrumentalizar a informação ou de que não consigam obter algum sucesso a partir dela. Embora as análises sobre a incerteza ser elemento central na teoria realista, é um equívoco o posicionamento de que a desconfiança invalidaria qualquer tipo de sinal de comunicação emitido por atores externos e de que eles sempre seriam recebidos com descrença. Outro ponto importante, que é contrário ao argumento de que a incerteza impossibilita as campanhas de informação, é o de que os Estados possuem aspectos internos que podem favorecer a penetração desses sinais.

Em resumo, o campo das teorias das Relações Internacionais ainda carece de explicações robustas em relação às campanhas de desinformação ou sobre o uso da informação para fins políticos. Como eco desse contexto, são necessários o desenvolvimento de análises que possam construir modelos teóricos capazes de abarcar o tema nas interações complexas entre atores no sistema internacional.

Subversão e RI

Na busca por uma teorização nas RI, destacam-se a perspectiva sobre a subversão como a reversão do poder estrutural e como instrumento estratégico (Maschmeyer 2022; Maschmeyer 2023; Krieg 2023). Os atores que detêm o poder estrutural possuem a capacidade de criar as estruturas de interação e as formam com o intuito de garantir vantagens. A subversão busca a exploração da estrutura do alvo para converter vantagens em prejuízos para quem detém o poder estrutural. As vulnerabilidades das regras e práticas da estrutura, tal como os agentes que interagem nas instituições e através delas, também são exploradas pela subversão. As operações de subversão

também podem ter como objetivo atingir os entendimentos de identidades constitutivas compartilhadas.

Dois fatores importantes determinam os efeitos que as atividades de subversão podem causar: a posição estrutural da entidade-alvo e a profundidade da subversão. Quanto ao primeiro fator, é preciso considerar que o poder subversivo não consegue mudar as posições estruturais, mas pode explorá-las de acordo com os seus interesses. Consequentemente, é necessária a realização de uma avaliação sobre os alvos possíveis para o sucesso das operações, através do esforço de influenciar a opinião pública a partir da disseminação de desinformação na mídia. Segundo, a profundidade da subversão depende principalmente da capacidade do perpetrador. Ao tentar subverter um adversário, é necessário identificar as vulnerabilidades e também elaborar as melhores formas de explorá-las. Para reverter o poder estrutural é necessária alguma familiaridade com o tipo de estrutura que se busca atingir, dessa forma, os Estados que possuem estruturas e níveis de poder estrutural semelhantes aos alvos, possuem menos barreiras que os que não apresentam essas condições (Maschmeyer 2022, 88).

Por seu turno, Krieg (2023) concebe a subversão como uma ferramenta estratégica. Difere-se quanto a Maschmeyer (2022, 2021) ao procurar relacionar a subversão e a guerra, a partir da abordagem tradicional de Clausewitz. Krieg aponta que a caracterização da subversão como um instrumento de poder orquestrado por redes de informação em coordenação, sem a presença de operações militares convencionais, parece ser incompatível com as definições de guerra tradicionais. A subversão busca a mudança do comportamento dos oponentes, mesmo sem o emprego de meios de coerção, distorcendo os limites entre a guerra e a paz. Também visa a exploração das vulnerabilidades sócio-psicológicas, físicas e infra-estruturais do ambiente informacional do alvo, para alterar o consenso sócio-político. Desse modo, a funcionalidade estratégica está em direcionar a consciência individual e de massa e, em casos mais extremos, causar a mudança de regime.

Para Krieg (2023, 73), as narrativas são determinantes na subversão, pois constroem realidades, fabricam identidades a indivíduos de uma comunidade e funcionam como enredos que se beneficiam "das fraquezas sociopsicológicas de forma a produzir a verdade como um fenômeno socialmente construído".[2] Essa utilização estratégica das narrativas em um contexto de subversão é classificado como 'armamento de narrativas'. Elas possuem como objetivo a alteração dos níveis de comunicação entre governantes e governados e a mudança nos padrões de comunicação entre diversos atores que coexistem

2 Tradução minha.

no processo decisório, como a imprensa, academia, sociedade civil e políticos. Para ser considerada como subversiva, a narrativa instrumentalizada como arma deve ser capaz de produzir mobilização e fabricar um alto nível de orquestração social através de diversos tipos de redes, e galvanizar o ativismo violento para obrigar reações por parte das lideranças políticas.

A mobilização é estruturada no caos do ecossistema informacional com informações falsas disseminadas de forma intencional ou não intencional. A consequência é a de que torna-se quase impossível filtrar as informações para se chegar a decisões políticas. Além disso, a incapacidade da política quanto à tomada de decisões efetivas diminui relativamente a confiança e a legitimidade dos órgãos do governo e polariza o discurso público. Nesse caso, os questionamentos levantados sobre as incapacidades do governo em lidar com a causa pública podem provocar violência política através de insurgências, por exemplo.

Sobre a vulnerabilidade dos Estados quanto aos impactos derivados de atividades de desinformação, Lanoszka (2019) aponta que essas ações não possuem efetividade, pois deveria refutar três hipóteses para serem exitosas: H1) a anarquia internacional gera incertezas sobre quaisquer informações transmitidas pelos adversários, logo os governos rivais sempre irão esperar as piores ações dos inimigos e vão construir meios de proteção em relação a elas; H2) os cidadãos geralmente confiam mais nas suas experiências prévias, possuem pré-conceitos sobre as elites políticas estrangeiras e seriam mais propensos a adotarem perspectivas ideológicas quando pensam sobre a dimensão internacional, do que as elites do Estado, fato que amplia a dificuldade de influência advinda de atores externos; H3) o Estado pode utilizar contramedidas mesmo em um cenário de polarização política, ele não é incapaz de tomar ações para reduzir os impactos das campanhas de desinformação e até mesmo desenvolver uma contra-campanha de desinformação para minimizar os danos da operação adversária.

Primeira hipótese

O primeiro motivo que reduz a efetividade das campanhas de desinformação é o fato de que a anarquia internacional produz incertezas sobre as informações provenientes dos adversários. Logo, os sinais de comunicação emitidos por atores externos sempre serão vistos de forma ambígua, pois não existe nenhum tipo de certeza sobre a natureza das ameaças e o que pode ser feito para combatê-las. Para que a campanha de desinformação seja bem-sucedida na missão de influenciar a sociedade e desestabilizar o processo

político, é preciso considerar que os indivíduos aceitariam qualquer tipo de informação externa. Para testar essa hipótese no caso brasileiro, é necessário identificar como o país geralmente recebe e interpreta as informações transmitidas por atores externos e também analisar o nível de penetração das mídias de outros Estados no ambiente da imprensa brasileira.

Embora não se restrinjam à internet, os principais esforços articulados de desinformação nos últimos anos foram realizados no ambiente virtual, sobretudo através de redes sociais (Rid, 2020). Lanoszka concorda com essa tendência ao enfatizar o fato da Rússia ter aumentado suas atividades na internet e o caso da Cambridge Analytica capturando dados do Facebook para serem utilizados nas campanhas da eleição presidencial nos EUA em 2016. Nas primeiras décadas do século XXI, observa-se, no Brasil, um crescimento astronômico do número de usuários de redes sociais, de mensageiros e de plataformas de streaming de vídeo. Esses serviços são fornecidos por poucas corporações que oligopolizam esse setor. Por exemplo, o Instagram e o Facebook, as maiores redes sociais em número de usuários no Brasil, pertencem ao mesmo grupo empresarial: Meta Inc. Mais ainda, o WhatsApp, o aplicativo de mensagens mais utilizado pelos brasileiros, com larga vantagem em relação aos concorrentes, também pertence ao mesmo conglomerado do Instagram e do Facebook.

O Google, o Android, o Gmail e o Chrome são, respectivamente, o buscador, sistema operacional de dispositivos móveis, o servidor de e-mail e o navegador mais utilizados no Brasil. Todos eles pertencem ao conglomerado Alphabet Inc., conhecido por ser o grupo empresarial que detém a maior quantidade de dados de indivíduos espalhados pelo mundo, controlando mais de 90% do mercado brasileiro de sites de busca. O YouTube, maior plataforma de streaming do planeta e a mais usada no Brasil, também é da Alphabet.

Essa concentração da internet brasileira em basicamente duas empresas dos EUA revelam uma incerteza, não só sobre a segurança das informações dos cidadãos do país pela posse de dados sensíveis por parte das companhias, mas também sobre a seleção do conteúdo acessado por usuários, que é definido por algoritmos controlados por pouquíssimos atores. Por exemplo, o algoritmo do Instagram e do Facebook seleciona alguns tipos de publicações para aparecerem na seção primária (feed) dessas redes sociais e costuma a dar destaque para temas considerados polêmicos e que geram certo tipo de engajamento. Esse tipo de processo é acompanhado pela possibilidade de disseminar informação com determinado viés a partir de um efeito manada. Dessa maneira, quanto menor a diversidade de corporações que prestam serviço no setor das redes sociais ou do armazenamento de dados, maior é a possibilidade de canais de disseminação de desinformação.

Ademais, a inexistência de empresas nacionais atuantes nessa área também amplifica o cenário de incerteza.

A título de exemplo, antes mesmo do início da guerra com a Ucrânia (2022), a rede social mais utilizada pelos cidadãos russos era a VK, uma empresa privada nacional. Os conflitos com Kiev e a piora das relações entre Moscou e o Ocidente fizeram o Facebook ser proibido no país. Já no mercado dos buscadores, a Google perde para a Yandex e o Telegram também ultrapassou o WhatsApp como o mensageiro mais popular. Algo semelhante também ocorre na China, o WeChat, a Weibo e o Baidu, empresas chinesas, superam todas as suas concorrentes estrangeiras.

A alta concentração corporativa no setor das TICs, com o predomínio de empresas estrangeiras, somada ao fraco desempenho da indústria nacional e a falta de interesse político em desenvolver essa área da economia, levam à conclusão de que a primeira hipótese/obstáculo é contestável no caso brasileiro. O controle total dos dados dos usuários por parte dessas empresas e o oligopólio dos algoritmos de seleção de conteúdo, possibilita um campo de penetração informacional por parte de possíveis adversários, mais ainda, permite a utilização de dados sensíveis dos usuários, o que poderia trazer riscos à segurança nacional. Desse modo, a fabricação de identidade e de sentido em uma comunidade se torna factível graças à capacidade de gerenciamento por parte dessas corporações sobre o que chega até o usuário dos seus serviços (Krieg 2023). Esse cenário também reflete o papel do ator subversivo, definido por Maschmeyer (2022), na exploração da estrutura alvo para converter as vantagens existentes do ecossistema informacional do Brasil (poder estrutural) em prejuízos.

A construção de um ambiente informacional seguro e a obtenção de vantagens estratégicas passa também pela análise das áreas da economia que são relacionadas ao setor tecnológico e ao debate sobre a segurança nacional. Consequentemente, a quantidade de recursos e o crescimento econômico podem ser positivos ao poder militar e a falta deles pode produzir vulnerabilidades à segurança estatal (Knorr 1977). Uma das suas considerações que mais impactam esta pesquisa certamente são as relacionadas à importância da inovação tecnológica no potencial econômico militar. Se a expansão da produção for mais estruturada no desenvolvimento tecnológico, traduzido na maior produtividade do trabalhador, do que no simples crescimento econômico, ela terá maiores benefícios quanto ao potencial militar, pois as atividades econômicas que envolvem alta tecnologia possuem mais sinergias em relação à indústria militar (Knorr 1973).

Para aumentar o potencial econômico-militar de um Estado, torna-se indispensável investimentos públicos em Pesquisa e Desenvolvimento.

Isso pode ser comprovado ao observar a parcela de gastos mundiais na área, que estão substancialmente concentrados nos países mais desenvolvidos em termos industriais, com destaque para a Pesquisa e Desenvolvimento no setor militar. Nesses termos, um Estado precisa associar a segurança nacional ao desenvolvimento dos seus setores de alta tecnologia relacionados ao nexo cibernético/informacional para, não só aumentar a produtividade industrial, mas também para potencializar a sua defesa contra ataques cibernéticos, construindo um ambiente de sinergia entre o desenvolvimento de setores estratégicos da economia e os meios de dissuasão contra esse tipo de influência. A inexistência de empresas nacionais nesse setor demonstra que o Brasil está longe de alcançar o nexo segurança-economia, pelo menos em termos da área da informação e comunicação.

Segunda hipótese

A hipótese de que os cidadãos confiam mais nas suas experiências prévias, possuindo pré-conceitos sobre as elites políticas estrangeiras e, por isso, seriam mais céticos à influência por parte de atores externos, também é contestável no caso do Brasil. Nessa hipótese, a relação entre o Estado e a sociedade geralmente afeta a forma pela qual o governo conduz a sua política externa. Entre essas duas partes, o acesso e o processamento de informação varia. Por exemplo, membros executivos envolvidos no processo de tomada de decisão em política externa possuem informações privilegiadas graças às instituições político-militares estatais que são controladas por esses agentes. Essas lideranças podem errar no processamento de informações, nos seus cálculos de poder relativo, na identificação de alternativas para lidar com os problemas e também na avaliação sobre as consequências de uma determinada ação (Lanoszka 2019).

Por outro lado, a sociedade não possui acesso a esse tipo de informação, tal como os decision makers. Quanto à visão sobre a condução da política externa, os cidadãos costumam confiar mais nas suas experiências, algo incomum para os envolvidos no processo de tomada de decisão nesse campo. Além disso, os cidadãos seriam mais propensos a adotarem perspectivas ideológicas, quando pensam sobre a dimensão internacional, do que as elites do Estado.

Na visão de Lanoszka (2019), as campanhas de desinformação têm como objetivo criar uma diligência entre os membros do executivo que estão envolvidos na política externa e o público em geral, de maneira a impactar o alinhamento do alvo no sistema internacional de acordo com os interesses

do Estado que empreende a operação. Para as operações de desinformação serem efetivas, deve-se levar em consideração a capacidade dos indivíduos influenciarem as políticas do Estado.

No caso do Brasil, essa hipótese pode ser refutada através de um ponto de vista sociológico. Por exemplo, Souza (2020) destaca elementos histórico-estruturais que auxiliaram o processo de adestramento da classe média do país na reprodução de um discurso anticorrupção, que na prática acabou transbordando o seu sentido. Esse processo histórico-estrutural está expresso na diferença ontológica entre seres humanos, sendo a base da vida política e social. Ele se traduz na ideia de que existe uma solução irrefutável para a vida social e política do mundo, portanto, essa resposta passa a ser tratada como sólida e impossível de ser contestada. Para isso, essa solução deve ser aceita como conhecimento científico universalmente válido, definindo o que é verdade e o que não é.[3]

Os controladores dessas definições sobre a validade do conhecimento, também costumam decidir o que é justo e o que é injusto e, portanto, podem justificar qualquer tipo de relação de dominação social e política.

No contexto público, a competição pelo sucesso da mensagem científica se dá através do acesso a investimento em recursos e em relações pessoais poderosas, a partir da dimensão simbólica das ideias e da sua efetividade na vida social. O Estado-nação moderno surge no contexto científico e na necessidade da legitimação e se traduz em pressuposições de identidade como a ideia de "povo eleito" e "nação escolhida", como é o caso dos EUA, que detém recursos para fortalecer esses discursos. Em países como o Brasil, onde uma elite colonizada que teve e tem a sua riqueza construída pelo trabalho de intermediação e pela exploração dos comandados, a identidade nacional não assume o sentido de "nação escolhida", mas sim de "vira-lata". A identidade brasileira é a imagem negativa da identidade americana: enquanto os americanos são percebidos como melhores, os brasileiros se percebem como os piores e os mais corruptos.

A elite brasileira colonizada reflete essa identidade. Ela cria a sua própria ciência a partir da prática e transforma um conhecimento existente de acordo com os interesses das grandes empresas e de governos, indicando quais saberes serão hegemônicos. Nesse processo de adequação, a elite brasileira é profundamente influenciada pela americana, em um processo relacional que tem como meta a expansão do capital estadunidense. A partir

3 Souza (2020) aponta que grande parte dessa ideia de conhecimento científico como verdade absoluta se dá através da percepção histórica iluminista da produção do conhecimento desvinculada de qualquer setor ou visão política. Esse arcabouço vem da visão de continuidade entre religião e ciência, presente no Ocidente. .

disso, o complexo de vira-lata abre a cognição dos indivíduos para a influência externa. Essa tendência aponta para uma instrumentalização da própria elite por atores estrangeiros.

Penido e Stédile (2020, 44) também destacam as tentativas de colonização do pensamento estratégico do Sul, que se dá através da estruturação de ações de cooperação, de treinamento e de formação que envolvem as forças armadas dos EUA e as de outros países da América Latina. Dentre as propostas, destacam-se: as metas orçamentárias para a indústria de defesa incompatíveis com as necessidades de desenvolvimento locais, a transformação das forças armadas latino-americanas em forças policiais, sobretudo com o crescimento das ações militares no combate ao crime organizado, e a manutenção de bases militares físicas dos EUA na região. Enquanto isso, internamente, Washington não segue essas medidas que são propagadas para o resto. Os Estados com pouca capacidade de investimento continuam apostando em estratégias equivocadas que acentuam o seu status de dependência estratégica. Os aspectos de subordinação e dependência das elites possibilitam que os movimentos de disseminação de desinformação tenham como sustento instituições no aparelho estatal, sem a morfologia de uma classe política nova ou de um novo movimento social.

Sobre as predisposições dos indivíduos, é importante mencionar que as narrativas exploram as fraquezas sociais e psicológicas da sociedade (Krieg 2023, 73). São atalhos metaheurísticos que criam sentido e dividem o mundo em bom/mau e legítimo/ilegítimo. Para a formação dessas narrativas armadas, considera-se a polarização política pré-existente, os cismas no tecido social e outras potencialidades de tensão. Por essas razões, além do fato do setor de informação e comunicação ter grande influência externa, as fraturas internas do Brasil são um grande sinal de vulnerabilidade para campanhas de desinformação.

Terceira hipótese

A terceira hipótese de Lanoszka (2019) é a de que o Estado pode utilizar contramedidas para minimizar as consequências das operações. O Estado não é um objeto inerte sem capacidade de tomar decisões para reduzir a força das operações de desinformação. Além disso, o Estado pode contra-atacar com o mesmo modus operandi.

Essa tomada de contramedidas passa por alguns processos de decisão na arena política. Lanoszka menciona que a necessidade de uma rápida capacidade de resposta para desmentir a desinformação é determinante para a

minimização das consequências. Entretanto, na propagação da desinformação na atual revolução digital, como afirma Rid (2020), torna-se extremamente complexo identificar o perpetrador. Outro problema, é que as contramedidas geralmente utilizadas, como os sites de verificação de fatos ou a punição dos atores internos que divulgam as desinformações, geralmente se concentram em diminuir os danos causados ao alvo. Pela velocidade de espalhamento propiciada pelas tecnologias da internet, a contenção de danos não é capaz de acompanhar a dinamicidade das operações de desinformação.

No que tange a dimensão institucional e considerando as interações entre a segurança da informação e o setor cibernético, no Brasil, a concepção estratégica sobre o ciberespaço ganhou seus primeiros contornos na Política Nacional de Defesa (2005) e na Estratégia Nacional de Defesa (2008). Esse último posiciona a cibernética como um setor estratégico em que o Exército possui a principal responsabilidade. Nos anos posteriores, outras interações entre os documentos se tornam concretas, como a elaboração exploratória, em 2010, de um livro verde de defesa cibernética e uma doutrina em 2014.

Estes documentos serviram de base para a construção das estruturas de defesa cibernética do Brasil, como o Centro de Defesa Cibernética (CDCiber) em 2012, a Escola Nacional de Defesa Cibernética (ENaDCiber) criada em 2015 e o estabelecimento do serviço em conjunto envolvendo o Comando de Defesa Cibernética, estabelecido em 2016, responsável pela defesa cibernética estratégica, e o CDCiber exercendo função operacional. A institucionalização estratégica do poder militar perpassa o CDCiber na função de estabelecer o Destacamento Conjunto de Defesa Cibernética cujo objetivo é prover as capacidades para guerra cibernética que serão conduzidas em nível tático pelo Destacamento Conjunto de Guerra Cibernética.

Em 2018 foi instituída a Política Nacional de Segurança da Informação (PNSI), com reformas na estrutura do país para cibersegurança e ciberdefesa. O novo modelo define a Segurança da Informação como uma área sistêmica que abrange a cibersegurança, a defesa cibernética, a segurança física e a proteção de dados. A PNSI designa o Gabinete de Segurança Institucional (GSI) como o administrador da cibersegurança e executor do planejamento da política de segurança da informação ao lado do Ministério da Defesa (MD).[4]

O documento prevê que o MD deve prestar apoio ao GSI nas atividades associadas à cibersegurança, além disso, deve construir diretrizes e procedimentos que podem ser utilizados nos sistemas ligados à defesa cibernética do país. Para Devanny et al. (2022, 7), essa mudança no modelo institucional aumenta o nível de prioridade da segurança cibernética, enquanto

4 Principalmente o Exército Brasileiro (EB), que é o responsável pela defesa cibernética. .

relega um papel de segundo plano para a defesa cibernética.

O PNSI também cria a Estratégia Nacional de Segurança da Informação (ENSI) que prevê o seu desenvolvimento em cinco módulos: segurança cibernética, defesa cibernética, segurança de infraestruturas críticas, segurança de informação confidencial e proteção contra vazamento de dados. A elaboração dos módulos ainda está em andamento e, atualmente, somente o de segurança cibernética foi publicado através do E-Ciber (Estratégia Nacional de Segurança Cibernética). O E-Ciber reforça o fato do comando da cibersegurança ser do GSI e o da defesa cibernética ser do MD.

A E-Ciber aponta uma série de objetivos estratégicos para o Brasil no setor de segurança cibernética. O primeiro é tornar o país mais próspero e confiável no ambiente digital. O segundo é aumentar a resiliência do país às ameaças cibernéticas. Por último, o terceiro objetivo é o fortalecimento do papel do Brasil na área de segurança cibernético em âmbito internacional.

Devanny et al (2022, 9) destacam que, apesar do estabelecimento desses marcos, há uma espécie de confusão conceitual, com a inexistência de uma definição clara para poder cibernético, aliada à tensão institucional principalmente devido à mudança de foco organizacional em direção à segurança cibernética promovida pelo PNSI. Dessa maneira, o poder cibernético não é utilizado como um conceito de integração estratégica nacional para tentar unificar os esforços que existem de forma separada para possibilitar a cibersegurança e defesa cibernética. Apesar dessas distorções, é importante ressaltar que o Brasil prioriza, pelo menos nessas publicações, que o desenvolvimento de capacidades cibernéticas defensivas e ofensivas, somada à construção de uma base industrial de defesa cibernética são prioridades. O E-Ciber ressalta a demanda de se fomentar parcerias entre a academia e os setores público e privado, bem como a necessidade de cooperação internacional para fins estratégicos.

Outro mecanismo construído pelo Brasil com o intuito de garantir a segurança da informação do Estado é o decreto nffl 11.856, de 26 de dezembro de 2023, estabelecendo a Política Nacional de Cibersegurança (PNCiber) e o Comitê Nacional de Cibersegurança. Estabelece os princípios, objetivos e instrumentos da Política Nacional de Cibersegurança e versa sobre a competência e a composição do Comitê Nacional de Telecomunicações.

Os objetivos da PNCiber são a promoção do desenvolvimento de produtos, serviços e tecnologias de caráter nacional destinados à segurança cibernética; a garantia da confidencialidade, autenticidade e disponibilidade das soluções e dos dados utilizados no processamento, armazenamento e transmissão eletrônica/digital de informações; incentivar o cuidado na atuação de crianças, adolescentes e idosos no ciberespaço; contribuir no combate ao

crime cibernético e outras ações maliciosas; incentivar o emprego de medidas de proteção cibernética e de gestão de riscos para prevenção, mitigação e neutralização de vulnerabilidades e ataques cibernéticos; promover a resiliência de entidades públicas e privadas quanto a ataques cibernéticos; promover a capacitação em segurança cibernética na sociedade; contribuir com as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança cibernética; incentivar a coordenação e o intercâmbio de informações de segurança cibernética entre os entes federativos, os três poderes, o setor privado e a sociedade; criar dispositivos de regulação, fiscalização e controle com o intuito de aprimorar a segurança cibernética nacional e desenvolver estratégias de cooperação em segurança cibernética (Brasil 2023).

No contexto das Forças Armadas e a sua relação com o poder cibernético, Devanny et al. (2022) destacam que, apesar de ser designado como um setor estratégico no documento da Estratégia Nacional de Defesa, o percentual destinado à área no orçamento do Plano de Articulação de Equipamento e Defesa é de apenas 1,48% comparado a outros programas do Exército. Entretanto, é importante destacar que o custo de entrada para tecnologias associadas ao poder cibernético é relativamente menor em comparação a outras capacidades militares, porém, em 2019, o orçamento de defesa cibernética praticamente dobrou de média em comparação ao período entre 2012 e 2018.

Quanto às redes sociais, há um crescimento do debate quanto à regulamentação das plataformas, principalmente no bojo da depredação das sedes dos três poderes no dia 8 de janeiro de 2023, pois grande parte dos responsáveis foi mobilizada através desses sites. Um exemplo relevante é a retomada das discussões sobre o projeto de lei 2630/2020, a chamada PL das Fake News, para controlar a disseminação de desinformação nessas redes. As discussões em torno da regulamentação ainda são bastante embrionarárias e possuem oposição importante, tanto por parte das corporações, como a Meta. e a Google, quanto por grupos de direita, alguns deles conhecidos por proliferarem desinformação nas mídias sociais. Apesar disso, em pesquisa publicada pela Atlas Intel em abril de 2023, 78% dos brasileiros defendem a necessidade de uma legislação que estabeleça regras bem definidas para a atuação das mídias sociais no país (Atlas Intel, 2023).

Na arena jurídica, o Brasil tem produzido algumas contramedidas e atividades de prevenção no que tange ao combate à desinformação. Como mencionado, o processo eleitoral brasileiro convive com a propagação de desinformação desde a popularização das redes sociais, tendo o seu ápice nas eleições de 2018 e 2022. O Tribunal Superior Eleitoral (TSE), desde 2019,

tem adotado uma série de medidas no combate à desinformação. Essas ações focam em campanhas visam a credibilização da Justiça Eleitoral. Para as eleições de 2022, foi criado o Programa Permanente de Enfrentamento à Desinformação, através da portaria nffl 510, de 4 de agosto de 2021 (TSE 2021) e foram adotadas uma série de medidas contra notícias falsas e perfis que propagam esse tipo de conteúdo, além de punições contra as redes sociais que mantinham essas informações online. Estas medidas trouxeram uma série de críticas em relação à diminuição dos direitos à liberdade de expressão, principalmente das corporações multinacionais que atuam no país.

Em virtude do que foi analisado nesta seção sobre a terceira hipótese, pode ser afirmado que o Brasil tem adotado algumas contramedidas institucionais quanto às campanhas de desinformação. Isso não quer dizer que o país possui um ambiente completamente seguro em relação a esse problema. Ainda há diversas críticas que podem ser realizadas, principalmente sobre a defasagem do sistema de inteligência nacional, mas percebe-se que essa hipótese é a que mais é corroborada no caso brasileiro. Certamente, o país não é estático no combate à desinformação e tem colocado em prática uma série de ações de combate e prevenção.

Conclusão

Esta pesquisa foi realizada de forma a analisar a efetividade das campanhas de desinformação no contexto do Brasil e discutir as políticas desenvolvidas pelo Estado na redução dos impactos desse tipo de operação. Dessa maneira, foi necessário identificar as vulnerabilidades do Brasil em relação à possibilidade de ser alvo de operações de desinformação promovidas por atores estatais ou não-estatais. Para isso, foram utilizadas as hipóteses/obstáculos construídas por Lanoszka (2019) em artigo publicado no European Journal of International Security, com o título 'Disinformation in International Politics'. Em sua análise, o autor busca corroborar o argumento de que as campanhas de desinformação não são efetivas, pois há diversos limites para o sucesso delas. Entretanto, as hipóteses criadas por Lanoszka (2019) corroboram o pressuposto da inefetividade se aplicadas apenas às grandes potências ou a Estados que possuem o setor das TICs relativamente estabelecido, e procuram despender esforços em segurança cibernética, através do desenvolvimento dessa área importante para a estratégia nacional.

Nesta presente pesquisa, através da testagem das três hipóteses no caso brasileiro, verificou-se que as duas primeiras falharam e a terceira foi corroborada de forma parcial. Na primeira, a alta concentração no setor das

TICs em empresas estrangeiras, além da presença incipiente da indústria nacional e da falta de interesse político nessa área da economia, indicam que o Brasil é vulnerável a campanhas de desinformação. Como mostrado a partir de dados sobre o setor das TICs, o Brasil ainda possui números bem menores, em termos de incentivo ao desenvolvimento nacional nessa área, em comparação a outros Estados em desenvolvimento, como a Índia. A falta de controle estatal sobre o algoritmo dessas empresas e a captação de dados sensíveis dos usuários por parte das corporações também ressaltam os riscos à segurança nacional. A maior parte dos serviços de internet são disponibilizados pelas big techs estadunidenses: Meta, Alphabet e Microsoft.

A segunda hipótese também é refutada, pois a sociedade brasileira possui predisposições internas que aumentam a probabilidade de sucesso de operações de desinformação, como a polarização política e a influência cultural externa. A polarização é traduzida, não apenas por eleições muito disputadas, mas pelo crescimento do discurso moral de condenação entre grupos, sobretudo a partir da ideia da existência de representantes da moral contra um grupo corrupto que passa a ser responsabilizado por todos os males sociais. Já a influência cultural externa se manifesta na experiência colonial que impede o desenvolvimento de um pensamento autônomo nacional e dita percepções como a corrupção inata na sociedade brasileira e a primazia ocidental.

Por último, através da testagem da terceira hipótese, pode-se afirmar que o Brasil cumpre parcialmente com os requisitos propostos por Lanoszka neste último obstáculo. Existe uma série de mecanismos que preveem contramedidas por parte das autoridades do país quanto à segurança da informação e segurança cibernética, como o PNSI e PNCiber. Também surgem medidas preventivas no escopo do Tribunal Superior Eleitoral para tentar preservar o transcurso das eleições. Há também um crescimento considerável da conscientização da população sobre a necessidade da regulamentação das redes sociais quanto à proliferação de desinformação, o que poderia garantir mais alternativas de contramedidas.

É necessário o desenvolvimento de mais estudos que investiguem a efetividade desse tipo de instrumentalização da desinformação, bem como investigações que analisem o impacto da subversão como forma de política estratégica. Torna-se imprescindível conceber as diferenças entre Estados no que tange às capacidades de defesa em relação ao problema, pois grande parte da literatura sobre o tema se restringe às grandes potências e ignora o espaço de atuação dos Estados emergentes onde a tecnologia digital possui um papel de grande importância.

Referências

Atlas Intel. 2023. Pesquisa sobre o impacto das redes sociais no bem-estar e segurança dos brasileiros. https://cdn.atlasintel.org/95c2051e-cfcf-480d-b69b-d91c413bbd97.pdf.

Barnett, M. e R. Duvall. 2005. "Power in international politics". International Organization, v. 58, n. 1, 39-75.

Brasil. 26 dez. 2023. Presidência da República. Casa Civil. Decreto nffl 11.856. Disponíel em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm#:~:text=DECRETO%20N%C2%BA%2011.856%2C%20DE%2026,que%20lhe%20confere%200%20art.

Bunce, V. e A. Hozic. 2016. "Diffusion-proofing and the Russian invasion of Ukraine", Demokratizatsiya, vol. 24, n. 4.

Choucri, Nazli. 2012. Cyberpolitics in International Relations. Cambridge: MIT Press.

Claverie, B. e F. Du Cluzel. 2022. Cognitive warfare: the advent of the concept of cognitics in the field of warfare. NATO Collaboration Support Office.

Fallis, D. 2016. "What is disinformation?". Library Trends, v. 64, n. 3.

Knorr, K. 1973. Power and Wealth. New Jersey: Princeton University Press.

Knorr, K. 1977. "Economic Interdependence and National Security". Em Economic Issues and National Security. Kansas: Allen Press.

Krebs, R. e P. Jackson. 2007. "Twisting tongues and twisting arms: the power of political rhetoric". European Journal of International Relations, v. 13, n. 1.

Krieg, A. 2023. Subversion: the strategic weaponization of narratives. Washington, DC: Georgetown University Press.

Lanoszka, A. 2019. "Disinformation in international politics". European Journal of International Security, v .4, n. 2, 227-248.

Maschmeyer, L. 2021. "The subversive trilemma: why cyber operations fall short of expectations". International Security, v.46, n.2, 51–90.

Maschmeyer, L. 2022. "A new and better quiet option? Strategies of subversion and cyber conflict". Journal of Strategic Studies.

Maschmeyer, L. 2023. "Subversion, cyber operations, and reverse structural power in world politics". European Journal of International Relations, v. 29, n.1, 79-103.

Ministério da Defesa [Brasil]. 2023. Doutrina Militar de Defesa Cibernética – MD 31-M07. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31M07DoutrinaMilitardeDefesaCiberntica2Edi02023.pdf,

_____. 2020. Defense White Paper. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/estado_e_defesa/livro_branco/Versaodolivroemportugues2020.pdf.

Nichols, G. C. Leal e C.R. Corrêa. 2023. "A Guerra Cognitiva nas Redes Sociais e suas Implicações para a Segurança dos Estados". Revista da Escola Superior de Guerra, v. 38, n. 82, 101-121.

Penido, A e M. E. Stédile. 2021. Ninguém regula a América: guerras híbridas e intervenções estadunidenses na América Latina. São Paulo: Expressão Popular/Fundação Rosa Luxemburgo.

Rid, T. 2020. Active Measures: The Secret History of Disinformation and Political Warfare. New York: Farrar, Straus and Giroux.

Rosenbach, E. e K. Mansted. 2019. "The Geopolitics of Information". The Belfer Center for Science and International Affairs.

Souza, J. 2020. A guerra contra o Brasil: como os EUA se uniram a uma organização criminosa para destruir o sonho brasileiro. Rio de Janeiro: Estação Brasil.

Stassun, C. e S. Assmann. 2012. "Hipermobilidade estética e dispositivos de controle de circulação: o desejo de ser notado encontrado na internet". Revista FAMECOS, Porto Alegre, v. 19, n. 2, 153-168. https://doi.org/10.5007/1984-8951.2012v13n102p153.

Strange, S. 1998. States and Markets. London: Bloomsbury Academic.

Suppo, H. R. 2011. "A importância do chamado soft power no paradigma realista clássico". Mural Internacional, v .2, n. 2, 47–50.

TSE. 2021. Secretaria de Gestão de Informação e do Conhecimento. Portaria nffl 510. Brasília. https://www.tse.jus.br/legislacao/compilada/prt/2021/portaria-no-510-de-04-de-agosto-de-2021.

Ventre, Daniel (ed). 2013. Cyber Conflict: Competing National Perspectives. Hoboken: John Wiley & Sons.

RESUMO
Algumas das maiores preocupações sobre a segurança da informação nas Relações Internacionais são os impactos da desinformação no processo político interno de forma a enfraquecer Estados adversários. Alguns estudos têm apontado para a falta de efetividade desse tipo de articulação em produzir resultados significativos na alteração do comportamento dos alvos. À luz desse pressuposto, esta pesquisa buscou testar, no caso do Brasil, três hipóteses que contestam a efetividade desse tipo de instrumento. Conclui-se que o país se encontra em uma situação de vulnerabilidade estratégica, mas tem movido esforços institucionais para contornar as possíveis consequências de uma campanha de desinformação.

PALAVRAS-CHAVE
Desinformação, Subversão, Segurança da Informação, Brasil

Recebido em 21 de janeiro de 2024
Aprovado em 30 de janeiro de 2025