MARINHA DO BRASIL
ESCOLA DE GUERRA NAVAL
DOUTORADO PROFISSIONAL EM ESTUDOS MARÍTIMOS

GISELLI CHRISTINA LEAL NICHOLS

GUERRA COGNITIVA NAS REDES SOCIAIS: ANÁLISE DAS AMEAÇAS E PROPOSTAS PARA POLÍTICAS PÚBLICAS DO MINISTÉRIO DA DEFESA

RIO DE JANEIRO
2024

GISELLI CHRISTINA LEAL NICHOLS

GUERRA COGNITIVA NAS REDES SOCIAIS: ANÁLISE DAS AMEAÇAS E PROPOSTAS PARA POLÍTICAS PÚBLICAS DO MINISTÉRIO DA DEFESA

Relatório Técnico apresentado ao Curso de Doutorado Profissional em Estudos Marítimos da Escola de Guerra Naval, como parte dos requisitos necessários à obtenção do título de Doutora em Estudos Marítimos.
Linha de pesquisa: Regulação do Uso do Mar, Processo Decisório e Métodos Prospectivos – LP II.
Área de Concentração: Defesa, Governança e Segurança Marítimas.
Orientador: CMG (RM1) IM Prof. Dr. Claudio Rodrigues Corrêa

RIO DE JANEIRO

2024

N616g Nichols, Giselli Christina Leal

Guerra cognitiva nas redes sociais: análise das ameaças e propostas para políticas públicas do Ministério da Defesa / Giselli Christina Leal Nichols.– Rio de Janeiro, 2024.

199 f. : il.

Relatório Técnico (doutorado profissional) - Escola de Guerra Naval, Programa de Pós-Graduação em Estudos Marítimos (PPGEM), 2024.

Orientador: Claudio Rodrigues Corrêa

Bibliografia: f. 172

1. Defesa Nacional. 2. Desinformação. 3. Guerra cognitiva. 4. Redes sociais. 5. Políticas Públicas. I. Escola de Guerra Naval.

CDD 320.951

Ficha catalográfica elaborada pela bibliotecária
Cremilda Santos - CRB7/3200
Biblioteca da Escola de Guerra Naval

GISELLI CHRISTINA LEAL NICHOLS

GUERRA COGNITIVA NAS REDES SOCIAIS: ANÁLISE DAS AMEAÇAS E PROPOSTAS PARA POLÍTICAS PÚBLICAS DO MINISTÉRIO DA DEFESA

Relatório Técnico apresentado ao Curso de Doutorado Profissional em Estudos Marítimos da Escola de Guerra Naval, como parte dos requisitos necessários à obtenção do título de Doutora em Estudos Marítimos.
Linha de pesquisa: Regulação do Uso do Mar, Processo Decisório e Métodos Prospectivos – LP II.
Área de Concentração: Defesa, Governança e Segurança Marítimas.
Orientador: CMG (RM1) IM Prof. Dr. Claudio Rodrigues Corrêa

Aprovado em 05 de julho de 2024.

Banca Examinadora

_____

Prof. Dr. Claudio Rodrigues Corrêa (PPGEM/EGN)
Orientador

_____

Prof. Dr. Adriano Lauro (PPGEM/EGN)

_____

Profª. Drª. Flavia Rodrigues de Castro (PPGEM/EGN)

_____

Prof. Dr. André Silva de Carvalho (Centro Universitário FEI)

_____

Prof. Dr. Sávio Antiógenes Borges Lessa (Faculdade Católica de Rondônia)

Dedico esta pesquisa de doutorado aos meus amados
David, Gabriella e Raphael, cujos apoio e encorajamento
foram a força motriz por trás deste desafio.

AGRADECIMENTOS

Primeiramente, agradeço a Deus por ter guiado os meus passos nessa jornada. Sua orientação e força foram fundamentais para superar os desafios e alcançar esta conquista.

Expresso minha profunda gratidão ao meu orientador, Prof. Dr. Claudio Rodrigues Corrêa (CMG RM1 IM), pela orientação excepcional e apoio constante ao longo deste projeto. Sua sabedoria e incentivo foram fundamentais para a realização deste trabalho.

Agradeço também aos membros da banca examinadora, Prof. Dr. Adriano Lauro, Profª. Drª. Flavia Rodrigues de Castro, Prof. Dr. André Silva de Carvalho e Prof. Dr. Sávio Antiógenes Borges Lessa, pela valiosa contribuição e sugestões que enriqueceram significativamente esta pesquisa.

Sou imensamente grata à minha família, que sempre me apoiou e compreendeu as demandas exigidas por este doutorado. Expresso minha mais profunda gratidão pelo amor, paciência e compreensão, e agradeço especialmente pela colaboração e pelo suporte moral durante os momentos desafiadores.

Por fim, a todas as pessoas e instituições que, de alguma forma, contribuíram para a realização deste trabalho, meus sinceros agradecimentos. Sua ajuda e apoio foram fundamentais para que eu pudesse concluir este desafio.

“Na guerra, a verdade é a primeira vítima”

Atribuída a Ésquilo

RESUMO

A guerra cognitiva é um fenômeno em crescimento, conduzido no domínio da mente humana, que está revolucionando a forma como as informações são compartilhadas e interpretadas nas redes sociais. A disseminação da desinformação e *fake news*, impulsionada por tecnologias avançadas como inteligência artificial (IA), algoritmos e *big data*, intensifica a complexidade dessas estratégias, com o propósito de manipular o pensamento e o comportamento dos indivíduos. A análise deste novo tipo de guerra e suas implicações globais orienta este estudo, cujo objetivo é fornecer subsídios para a formulação de políticas públicas pelo Ministério da Defesa (MD) contra as ameaças à Expressão Psicossocial do Poder Nacional decorrentes da guerra cognitiva nas redes sociais. Para alcançar esse objetivo, foi empregada uma abordagem de triangulação de métodos qualitativos, incluindo pesquisa bibliográfica, revisão da literatura, método *ex-post facto*, análise comparativa e *survey*. Esta pesquisa se destaca não apenas por sua inovação com o tema, mas também pela complexidade evidenciada por meio da integração de conhecimentos de diversas áreas. Os resultados demonstram que a manipulação da informação e das percepções públicas nas redes sociais é uma arma central da guerra cognitiva, explorando fragilidades do cérebro para influenciar emoções e comportamentos, e desestabilizar sociedades democráticas. Eventos recentes no Brasil ilustram como essa dinâmica se desenvolve, destacando vulnerabilidades significativas na Expressão Psicossocial do Poder Nacional. Diante da crescente influência da guerra cognitiva nas redes sociais e de suas implicações globais, este estudo oferece importantes contribuições para a formulação de políticas públicas de defesa nacional. Além disso, suas recomendações apresentam uma aplicabilidade concreta, delineando um conjunto de medidas executáveis.

Palavras-chave: Guerra cognitiva; Redes sociais; Desinformação; Defesa nacional; Políticas públicas.

ABSTRACT

Cognitive warfare is a growing phenomenon, conducted in the domain of the human mind, that is revolutionizing the way information is shared and interpreted on social networks. The dissemination of disinformation and fake news, driven by advanced technologies such as artificial intelligence (AI), algorithms, and big data, intensifies the complexity of these strategies, with the purpose of manipulating the thoughts and behavior of individuals. The analysis of this new type of warfare and its global implications guides this study, whose objective is to provide subsidies for the formulation of public policies by the Ministry of Defense (MD) against threats to the Psychosocial Expression of National Power resulting from cognitive warfare on social networks. To achieve this objective, a triangulation approach of qualitative methods was employed, including bibliographical research, literature review, ex-post facto method, comparative analysis, and survey. This research stands out not only for its innovation with the theme but also for the complexity evidenced through the integration of knowledge from various areas. The results demonstrate that the manipulation of information and public perceptions on social networks is a central weapon of cognitive warfare, exploiting brain vulnerabilities to influence emotions and behaviors and destabilize democratic societies. Recent events in Brazil illustrate how this dynamic develops, highlighting significant vulnerabilities in the Psychosocial Expression of National Power. Given the growing influence of cognitive warfare on social networks and its global implications, this study offers important contributions to the formulation of national defense public policies. In addition, its recommendations present a concrete applicability, outlining a set of executable measures.

Keywords: Cognitive warfare; Social networks; Disinformation; National defense; Public policies.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AEED	Assessoria Especial de Enfrentamento à Desinformação
AICHR	Comissão Intergovernamental de Direitos Humanos da ASEAN
AID	Atividade de Inteligência de Defesa
AMITT	*Adversarial Misinformation and Influence Tactics and Techniques*
ANPD	Autoridade Nacional de Proteção de Dados
ASEAN	Associação das Nações do Sudeste Asiático
BID	Base Industrial de Defesa
C,T&I	Ciência, Tecnologia e Inovação
CA	*Cambridge Analytica*
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CDO	*Cognitive Domain Operations*
CIA	*Central Intelligence Agency*
CMAG	Comitê de Monitoramento e Avaliação de Gastos Diretos
CMAP	Conselho de Monitoramento e Avaliação de Políticas Públicas
CMAS	Comitê de Monitoramento e Avaliação dos Subsídios da União
CNCIBER	Comitê Nacional de Cibersegurança
CNNS	Redes neurais convolucionais
CNPQ	Conselho Nacional de Desenvolvimento Científico e Tecnológico
CogWar	*Gognitive Warfare*
DATTI	Desinformação Adversarial, Táticas e Técnicas de Influência
DEP	Diretoria de Ensino e Pesquisa
DSN	Departamento de Segurança Nacional
EDAP	Plano de Ação para a Democracia Europeia
EI	Estado Islâmico
ELP	Exército de Libertação Popular
END	Estratégia Nacional de Defesa
ENINT	Estratégia Nacional de Inteligência
ERGA	Grupo de Reguladores Europeus dos Serviços de Comunicação Social Audiovisual
EUA	Estados Unidos da América
FBI	*Federal Bureau of Investigation*

FFAA	Forças Armadas
FIMI	*Foreign Information Manipulation and Interference*
FRENTE	Frente Nacional de Enfrentamento à Desinformação
G7	Grupo dos 7
IA	Inteligência artificial
IBICT	Instituto Brasileiro de Informação em Ciência e Tecnologia
IC	*United States Intelligence Community*
ICT	Científicas, Tecnológicas e de Inovação
IFCN	*International Fact-Checking Network*
IPEA	Instituto de Pesquisa Econômica Aplicada
ISIS	*Islamic State of Iraq and Syria*
JCDCLEPD	*Joint Declaration on Challenges for Freedom of Expression in the Next Decade*
KGB	*Committee for State Security*
LBDN	Livro Branco da Defesa Nacional
LGPD	Lei Geral de Proteção de Dados Pessoais
MCI	Marco Civil da Internet
MD	Ministério da Defesa
MIoP	*Military Instrument of Power*
MIT	*Massachusetts Institute of Technology*
MRR	Mecanismo de Resposta Rápida
NATO	*North Atlantic Treaty Organization*
NWCC	*NATO Warfighting Capstone Concept*
OEA	Organização dos Estados Americanos
OII	*Oxford Internet Institute*
ON	Objetivos Nacionais
ONGS	Organizações Não Governamentais
ONU	Organização das Nações Unidas
PAD	Plano de Ação contra a Desinformação
PCC	Partido Comunista Chinês
PCD	Programa de Combate à Desinformação
PDMAF	Programa Desportivo Militar Anual das Forças Armadas

PDN	Política de Defesa Nacional
PED	Programa de Enfrentamento à Desinformação
PEED	Programa Permanente de Enfrentamento à Desinformação
PID	Política de Inteligência de Defesa
PLASSF	*People's Liberation Army Strategic Support Force*
PNBID	Política Nacional da Base Industrial de Defesa
PNCIBER	Política Nacional de Cibersegurança
PND	Política Nacional de Defesa
PNI	Política Nacional de Inteligência
PNISP	Política Nacional de Inteligência de Segurança Pública
PNRM	Política Nacional para os Recursos do Mar
PNSPDS	Política Nacional de Segurança Pública e Desenvolvimento Social
POSIN-MD	Política de Segurança da Informação da Administração Central do Ministério da Defesa
PPA	Plano Plurianual
PROCAD	Programa de Cooperação Acadêmica
PROFI	Programa de Fortalecimento Institucional
PSGIC-DEF	Plano Setorial de Gestão de Incidentes Cibernéticos do Setor Defesa
PSYOPS	Operações Psicológicas
RHETOPS	*Rhetoric and Information Warfare*
RNNS	Redes neurais recorrentes
ROAM	*Rights, Openness, Accessibility, Multistakeholder*
SARS	Síndrome Respiratória Aguda Grave
SCL	*Strategic Communication Laboratories Group*
SEAE	Serviço Europeu para a Ação Externa
SEDIGI	Secretaria de Direitos Digitais
SENASP	Secretaria Nacional de Segurança Pública
SINDE	Sistema de Inteligência de Defesa
SISBIN	Sistema Brasileiro de Inteligência
STF	Supremo Tribunal Federal
STIX	*Structured Threat Information Expression*
TRE	Tribunal Regional Eleitoral

TSE	Tribunal Superior Eleitoral
UE	União Europeia
UNESCO	*United Nations Educational, Scientific and Cultural Organization*
VIGIA	Programa Nacional de Segurança nas Fronteiras e Divisas

SUMÁRIO

1 INTRODUÇÃO

A guerra cognitiva é um fenômeno emergente e complexo que está redefinindo a forma como as informações são disseminadas e percebidas nas redes sociais. Diferentemente das guerras tradicionais, onde a batalha ocorre no campo físico, a guerra cognitiva é conduzida no domínio da mente humana. Ela explora as vulnerabilidades do cérebro, manipulando emoções e percepções para alterar a maneira como as pessoas pensam e agem. Seu objetivo não é apenas persuadir, mas transformar o conhecimento em uma arma, relativizando a verdade e modificando a forma pela qual as pessoas processam informações e tomam decisões. As plataformas online têm sido um campo fértil para a disseminação dessas estratégias, onde a rapidez e a amplitude de alcance possibilitam uma influência sem precedentes sobre as percepções e comportamentos dos indivíduos (Bernal *et al*., 2020).

Em um movimento "insidioso", a guerra cognitiva utiliza desinformação, narrativas falsas e estratégias sofisticadas de manipulação da verdade, com o intuito de influenciar atitudes, comportamentos e crenças (Cluzel, 2020). A disseminação deliberada de informações falsas nas redes sociais tem o potencial de causar profundas transformações em valores e princípios, impactando significativamente a cultura de uma sociedade. Esse fenômeno se torna particularmente problemático quando a desinformação é direcionada para explorar divisões já existentes entre os indivíduos. Ao manipular narrativas e distorcer fatos, esses esforços visam não apenas desestabilizar a coesão social, mas também minar a confiança nas instituições democráticas. A guerra cognitiva, portanto, não se limita a impactar indivíduos de forma isolada, mas também objetiva desestruturar o tecido social e enfraquecer as bases da governança do Estado (Allcott; Gentzkow, 2017).

Em um mundo cada vez mais hiperconectado, onde a influência dos meios digitais no comportamento humano se tornou vital para as estratégias de poder, reconhecer a importância da guerra cognitiva como uma ameaça à integridade da informação e à estabilidade social é fundamental para manter a segurança e a soberania nacional (NATO, 2022). Diante dessa realidade, este Trabalho de Conclusão de Doutorado (TCD), apresentado como Relatório Final de Pesquisa, se propõe a examinar a natureza e as implicações da guerra cognitiva nas redes sociais e suas ameaças à Expressão Psicossocial do Poder Nacional brasileiro. Essa expressão diz respeito à interação entre os fatores psicológicos, sociais e ambientais que formam o bem-estar emocional e mental da população. Dentre as cinco dimensões[1] do Poder Nacional, é aquela

[1] Além da Expressão Psicossocial, as outras dimensões do Poder Nacional incluem a dimensão Econômica, que é a capacidade de gerar riqueza e controlar recursos; a dimensão Militar, que diz respeito à Força Armada e su

que tem relação com a socialização, o controle e a coesão do tecido social. Esses elementos são essenciais para um poder de Estado eficiente, que preze pelo bom funcionamento de uma sociedade, especialmente sob a perspectiva de sistemas democráticos (ESG, 2009). É importante destacar que, no contexto psicossocial do Poder Nacional dos Estados democráticos, o controle, conforme citado, busca o fortalecimento da sociedade e a participação cidadã nos processos de decisão e governança, ao contrário das práticas e mecanismos de regimes autoritários.

Para identificar as ameaças que a guerra cognitiva nas redes sociais pode significar à Expressão Psicossocial, são investigados, nesta pesquisa, os mecanismos subjacentes a essas operações, as motivações dos atores envolvidos e as iniciativas que visam combater essas ameaças. Contribuindo para aprofundar esse entendimento, o estudo também busca analisar como a desinformação e as campanhas de manipulação digital podem influenciar a opinião pública e comprometer a democracia, oferecendo recomendações para a formulação de políticas públicas no âmbito do Ministério da Defesa.

É importante reconhecer que, além dos riscos e desafios emergentes associados às redes sociais, essas plataformas também apresentam aspectos positivos. Ao promover as interações sociais, essas tecnologias possibilitam a formação de comunidades com base em interesses lícitos e comuns, contribuindo para o estabelecimento de vínculos benéficos e a geração de oportunidades de desenvolvimento de conhecimento e habilidades. Também facilitam o acesso a temas importantes que não estão disponíveis nos meios de comunicação tradicionais, entre outros atributos (Junqueira *et al*, 2014). Compreender e abordar os benefícios além dos riscos associados, é fundamental para garantir que essas plataformas sejam utilizadas ética e construtivamente. Esta pesquisa, entretanto, se concentra nas ameaças das operações maliciosas que exploram as vulnerabilidades das redes sociais, impactando a forma como as informações são disseminadas e percebidas pelos usuários.

1.1 CONTEXTO E TENDÊNCIAS DAS AMEAÇAS INFORMACIONAIS

Os últimos séculos foram marcados principalmente por ameaças à segurança física dos Estados, o que levou as forças armadas a responderem às guerras cinéticas com os meios tradicionais disponíveis (Parks; Duggan, 2011). No entanto, uma nova forma de Guerra Não

relação com a defesa do país; a dimensão Política, atuante na governança e na legitimidade do sistema político; e a dimensão Científica-Tecnológica, relativa à inovação e ao desenvolvimento de conhecimento e tecnologia (ESG, 2009).

Convencional (GNC)[2] tem se disseminado rapidamente no ambiente online, empregando uma variedade de operações, incluindo informacionais, psicológicas, cibernéticas e de engenharia social[3]. Com estratégias nem sempre identificáveis, a guerra cognitiva se dissemina velozmente nas redes sociais, explorando as vulnerabilidades do cérebro humano com o propósito de moldar tanto o pensamento quanto o comportamento, exercendo influência direta sobre a percepção e as ações dos indivíduos (Cluzel, 2020).

Em 2021, os chefes de Estado e de governo da Organização do Tratado do Atlântico Norte (OTAN, ou NATO na sigla em inglês) reconheceram a importância do campo cognitivo nas estratégias de defesa. O documento "*NATO Warfighting Capstone Concept (NWCC)",* referendado por esses executivos, aborda de forma particular os aspectos mais recentes da competição entre grandes potências diante das mudanças do caráter da guerra. O relatório enfatiza que "é fundamental entender como o MIoP[4] da Aliança deve conduzir futuros combates bélicos no ambiente operacional multirregional, multidimensional (físico, virtual e cognitivo) e multidomínio" (NATO, 2021b, p. 7, tradução nossa)[5]. Em um documento político posterior, que orienta a Aliança para a próxima década *"NATO 2022 Strategic Concept",* são ressaltados os aspectos relacionados à guerra cognitiva, como as atividades maliciosas no ciberespaço e campanhas de desinformação, entre as estratégias utilizadas por agentes maliciosos contra os processos e instituições democráticas (NATO, 2022a).

Nesse contexto de evolução das ameaças, em que a convergência de forças culturais, políticas e históricas tem transformado o ecossistema geopolítico de hegemônico para multipolar, os formuladores de políticas públicas enfrentam um dilema de segurança mais complexo e difuso, que até então estava subestimado. Incluídos nessa nova dinâmica, as redes sociais tornaram-se plataformas fundamentais para a exploração de questões culturais, econômicas, políticas, sociais e de outros temas diversos, encontrando no campo de batalha da mente um térreo fértil para exploração de fragilidades cognitivas individuais e coletivas. Essa mudança de eixo do poder associada às facilidades de disseminação de informação pelas plataformas online despertou no público interno a importância de temas de política externa, ao

2 Tipo de combate, em geral de longa duração, caracterizado pelo emprego de ações indiretas, diferentes das formas clássicas de organização e combate militar, sendo conduzido predominantemente por grupos irregulares, organizações paramilitares ou outras forças não convencionais (Brasil, 2016, p. 66).

3 Técnica relacionada à segurança da informação que utiliza a persuasão, manipulação e influência das pessoas, a fim de obter informações sigilosas (Mitnick; Simon, 1963).

4 O *MIoP (Military Instrument of Power)* é um conceito estratégico da OTAN que se refere ao conjunto de capacidades militares que a aliança utiliza para exercer influência e garantir a segurança em diferentes contextos.

5 "It is paramount to understand how the Alliance MIoP must conduct future warfighting in the multi-region, multi-dimensional (physical, virtual, and cognitive) and multi-domain operating environment".

mesmo tempo em que assuntos domésticos adquiriram uma dimensão global (Wilson III; Smitson, 2020).

Essas questões estão diretamente relacionadas ao comportamento dos indivíduos nas redes sociais e à forma como as informações pessoais são compartilhadas e absorvidas. Esse fenômeno, conhecido tecnicamente como "hipermobilidade estética dos internautas", contribui para que os agentes virtuais possam traçar o perfil do usuário com o propósito de segmentar o conteúdo e direcionar mensagens personalizadas para atrair atenção e engajamento e atingir a seus objetivos específicos. Ele se caracteriza por uma maior flexibilidade dos indivíduos no gerenciamento da privacidade devido à constante busca por reconhecimento e validação nas redes sociais. Esse comportamento licencioso leva à auto exposição excessiva de seus dados e imagens digitais, facilitando uma maior exposição às táticas de manipulação de informações (Stassun; Assmann, 2012).

Um exemplo dessa dinâmica foi a atuação da Cambridge Analytica no referendo do *Brexit (Britain+exit),* que ocorreu no Reino Unido em 2016. A empresa obteve indevidamente dados de milhões de usuários do Facebook e usou técnicas de microsegmentação para criar anúncios políticos personalizados, com o propósito de influenciar o resultado do referendo. Esse incidente destacou os riscos da coleta e uso não autorizados de informações pessoais para fins políticos e comerciais. A empresa também usou o mesmo método nas eleições presidenciais dos Estados Unidos de 2016, tentando influenciar os eleitores por meio de conteúdo direcionado. Esse episódio levantou preocupações sobre a ética e a legalidade do uso de dados pessoais para fins político-eleitorais, colocando em questão os limites da privacidade e a integridade do processo democrático (Cadwalladr, Graham-Harrison, 2018).

Estratégias semelhantes no uso das redes sociais foram adotadas por países como Rússia e China, gerando crescente preocupação na comunidade global. As agências de inteligência desses países desempenharam um papel proeminente na disseminação de desinformação, explorando as vulnerabilidades das redes sociais como um novo teatro de operações para a guerra cognitiva. Documentos e análises recentes, como os artigos de Barnes e Sanger (2020) e o estudo de Molter e DiResta (2020), destacaram esse fenômeno, enfatizando a urgência de compreender e combater essas estratégias de influência, interferência e alteração das dinâmicas cognitivas. Estudos como de Anwar (2022) sugerem uma potencial convergência de interesses e estratégias entre Rússia e China nessa área, indicando uma colaboração mais próxima. Essas estratégias impactam vários setores, incluindo política, segurança e sociedade em geral, conforme discutido por Kelton *et al* (2019).

Ozawa (2021), Kannenberg e Ortellado (2020) e Ricard e Medeiros (2020) relatam que. grupos de apoiadores do então candidato Jair Bolsonaro às eleições presidenciais brasileiras de 2018 utilizaram as mesmas estratégias na disseminação de notícias falsas *(fake news)* e discursos de ódio em massa nas redes sociais para influenciar a opinião pública e o voto dos eleitores. Essas táticas de propaganda digital, configuradas como parte de uma estratégia de guerra cognitiva, principalmente devido às suas características e ao impacto profundo na percepção e comportamento da população, ficaram conhecidas como o "escândalo das *fake news*".

Investigações posteriores indicaram que empresas especializadas em propaganda digital teriam sido contratadas pela campanha do candidato para criar e impulsionar conteúdo enganoso em larga escala, usando o *microtargeting* para direcionar esses materiais a segmentos específicos ao eleitorado. Essas táticas continuaram após a eleição, passando de uma "arma de campanha" para se tornarem uma ferramenta de propaganda governamental. Essas ações planejadas levantaram questões sobre a legalidade e a ética desse tipo de atuação, especialmente no contexto do processo eleitoral (Ozawa, 2021; Kannenberg, Ortellado, 2020; Ricard, Medeiros, 2020).

Essas práticas foram corroboradas pelo estudo do Oxford Internet Institute (OII), que revelou que o Brasil teve participação expressiva na disseminação de desinformação nas redes sociais. Grupos de agentes internos espalharam mensagens pró-governo, ataques à oposição e estimularam a polarização para influenciar debates políticos, eleições e a percepção da população. A pesquisa, realizada no período de 2016 a 2020 com 81 países, identificou que essas estratégias foram amplamente utilizadas em todo o mundo, revelando a participação do Brasil na guerra cognitiva (Bradshaw; Bailey; Howard; 2021).

O estudo também destacou que as "tropas cibernéticas" brasileiras operavam de forma permanente, com coordenação central e recursos financeiros significativos. Essas equipes utilizavam *fake news*, ataques a jornalistas e meios de comunicação com posicionamento editorial crítico em relação ao governo, além de perfis *hackeados* para disseminar conteúdo manipulado. A pesquisa incluiu o Brasil ao lado de outros 36 países que usaram a desinformação como estratégia nas redes sociais, como, por exemplo, a Armênia, Austrália, Bolívia, Cuba, Hungria, Polônia, México, Síria e Turquia (Bradshaw; Bailey; Howard; 2021).

Assim como no caso da Cambridge Analytica, Rússia e China, esses eventos no Brasil desafiaram os limites da privacidade, da liberdade de expressão e da integridade do sistema democrático. Eles evidenciaram a necessidade premente de regulamentação e fiscalização mais

efetivas sobre a coleta, o uso e a disseminação de dados pessoais em campanhas políticas, a fim de preservar a integridade do debate público e do voto.

Nesse novo contexto, onde a tecnologia avança rapidamente, faz-se necessário analisar as relações entre as novas tecnologias digitais informacionais e de relacionamento, e refletir sobre o aumento das ameaças da guerra cognitiva nas redes sociais nas próximas décadas, impulsionadas sua evolução tecnológica. As estratégias de desinformação e manipulação cognitiva, amplamente empregadas por agentes estatais e não estatais, revelam a fragilidade das instituições democráticas frente a essas novas formas de guerra. Episódios como o da Cambridge Analytica e a atuação de tropas cibernéticas no Brasil destacam a urgência de uma maior vigilância e entendimento sobre o uso de dados pessoais e a disseminação de informações manipuladas no ambiente online (Cadwalladr; Graham-Harrison, 2018; Bradshaw; Bailey; Howard, 2021). Do mesmo modo, a ação de países como Rússia e China, que têm desempenhado um papel proeminente na disseminação de desinformação, alertam para as vulnerabilidades das redes sociais e de sua configuração como um novo teatro de operações para a guerra cognitiva (Anwar, 2022; Molter; DiResta, 2020). A exploração dessas fragilidades cognitivas é um dos aspectos que evidencia um cenário onde a integridade dos processos democráticos é constantemente desafiada, exigindo uma resposta proporcional às novas ameaças que surgem no panorama geopolítico contemporâneo (Stassun; Assmann, 2012; Kelton *et al*., 2019).

Diante do momento político nacional estudado, marcado por intensa polarização e eventos significativos, a inclusão dos acontecimentos de 8 de Janeiro de 2023 na pesquisa foi uma decisão que, apesar de se reconhecer a possibilidade de questionamentos sobre a imparcialidade do estudo, ela se justifica por razões fundamentais. Primeiramente, omitir esses eventos significaria ignorar um episódio de grande relevância histórica e política, que foi abordado em diversas áreas de estudo, incluindo ciência política, sociologia e comunicação. Esses fatos, amplamente documentados por fontes oficiais, oferecem uma base sólida e factual para a análise crítica proposta.

Por outro lado, a exclusão desses eventos poderia ser interpretada como uma tentativa de minimizar ou ignorar a realidade dos desafios enfrentados pela sociedade brasileira contemporânea, comprometendo assim a integridade e a completude da análise. Embora essa abordagem possa levantar debates e controvérsias, o rigor acadêmico e a transparência na apresentação dos fatos foram preconizados com a finalidade de contribuir para um entendimento mais profundo e atualizado da realidade política e social do Brasil.

1.2 PROBLEMA DE PESQUISA

A expansão acelerada das redes sociais e a crescente digitalização da sociedade têm gerado novas oportunidades e desafios em vários aspectos da vida atual. Entretanto, ao lado dessas oportunidades, surgem também novas ameaças, particularmente no contexto da guerra cognitiva no meio digital. Marcada pela propagação de informações falsas, manipulação de dados e publicidade direcionada, a guerra cognitiva tem se mostrado um instrumento eficaz para moldar a opinião pública, formar percepções e manipular comportamentos.

Diante do complexo e dinâmico contexto da utilização das redes sociais como teatro de operações da guerra cognitiva, este TCD aborda o seguinte problema de pesquisa: As campanhas de desinformação e manipulação nas redes sociais representam ameaças para a Expressão Psicossocial do Poder Nacional?

1.3 HIPÓTESE

Esta pesquisa parte da hipótese de que as redes sociais podem ser empregadas estrategicamente como ferramentas de guerra cognitiva contra a Expressão Psicossocial do Poder Nacional brasileiro. Essa guerra cognitiva digital ocorreria por meio das campanhas de desinformação e manipulação da opinião pública, fomentando conflitos sociais, econômicos e políticos na sociedade brasileira.

Ao investigar essa hipótese, busca-se compreender melhor estratégias utilizadas nesse contexto, bem como identificar medidas eficazes para detectar, prevenir e mitigar esses impactos negativos, visando fortalecer a estabilidade, a segurança e a integridade da Expressão Psicossocial do Poder Nacional.

1.4 OBJETIVOS

1.4.1 Objetivo geral

Este estudo visa fornecer subsídios para a formulação de políticas públicas pelo Ministério da Defesa contra as ameaças à Expressão Psicossocial do Poder Nacional decorrentes da guerra cognitiva nas redes sociais.

1.4.2 Objetivos específicos

a) Identificar os tipos de guerra empregados no ambiente digital, com ênfase na guerra cognitiva online e seus aspectos constitutivos;
b) Analisar estratégias de atores estatais e não estatais utilizadas na guerra cognitiva nas redes sociais;
c) Investigar como essas estratégias podem afetar a Expressão Psicossocial do Poder Nacional brasileiro;
d) Analisar iniciativas de políticas públicas nacionais e internacionais de mitigação da guerra cognitiva nas redes sociais;
e) Apresentar recomendações para elaboração de políticas públicas no âmbito do Ministério da Defesa para enfrentamento da guerra cognitiva nas redes sociais.

1.5 JUSTIFICATIVA

A guerra cognitiva é um fenômeno complexo e sofisticado que está mudando o modo como as informações nas redes sociais são compartilhadas, percebidas e interpretadas. Em contraste às guerras físicas convencionais, essa nova forma de guerra é realizada no domínio da mente, explorando suas vulnerabilidades com o objetivo de remodelar processos de pensamento e comportamento, manipulando, desta forma, emoções e percepções.

Esse fenômeno levanta preocupações significativas, especialmente quando a desinformação é utilizada para explorar divisões que já existem na sociedade. Como um espectro da guerra híbrida, essa estratégia é empregada tanto por governos quanto por atores não estatais na manipulação de narrativas e distorção dos fatos, com objetivo não apenas de desestabilizar a coesão social, mas também enfraquecer a confiança nas instituições democráticas.

Em um mundo globalizado e conectado digitalmente, a crescente influência dos meios digitais no comportamento humano tem sido um fator crítico para o exercício do poder em várias áreas. Com o avanço da tecnologia, torna-se cada vez mais evidente que o modo de compartilhamento e percepção das informações desempenha um papel relevante na dinâmica social e política de uma nação.

Diante dessa realidade emergente, essa pesquisa se propõe a analisar a natureza e as implicações da guerra cognitiva nas redes sociais e suas ameaças à Expressão Psicossocial do

Poder Nacional brasileiro. O estudo investiga os mecanismos subjacentes a essas operações, as motivações dos atores envolvidos e as iniciativas que visam combater essas ameaças.

Além disso, a pesquisa busca analisar como a desinformação e as campanhas de manipulação digital podem afetar a opinião pública e comprometer a democracia, oferecendo recomendações para a formulação de políticas públicas no âmbito do Ministério da Defesa. A justificativa para a realização desta pesquisa de doutorado se baseia na necessidade de se entender a natureza complexa e dinâmica da guerra cognitiva, o seu impacto na estabilidade social e nos processos democráticos, contribuindo, desta forma, com subsídios para o desenvolvimento de estratégias contra essas ameaças.

Esse estudo científico está inserido na linha de pesquisa "Regulação do uso do mar, processo decisório e métodos prospectivos", na área de concentração "Defesa, Governança, e Segurança marítima" e da Linha de Pesquisa II "Regulação do uso do mar, processo decisório e métodos prospectivos" do Programa de Pós-Graduação em Estudos Marítimos da Escola de Guerra Naval (PPGEM/EGN). Sua abordagem atende à "complexa e dinâmica relação interestatal e seus possíveis desdobramentos até longo prazo" (Brasil, 2024c, s.p).

A pesquisa foi financiada com recursos do projeto "Prospectiva para Segurança e Defesa" do Programa de Cooperação Acadêmica em Defesa (PROCAD-Defesa), coordenado pela Escola de Guerra Naval (EGN), uma vez que sua temática está plenamente alinhada ao objetivo geral do projeto, que é "ampliar a compreensão sistêmica em temas de impacto em defesa e segurança pela integração das FFAA e sociedade, na pesquisa e monitoramento das sementes de futuro para os cenários de defesa do Brasil" (Corrêa, Janick, 2021).

O presente estudo adota uma abordagem metodológica qualitativa para compreender em profundidade o fenômeno da guerra cognitiva nas redes sociais e suas implicações para a Expressão Psicossocial do Poder Nacional brasileiro. A fim de reduzir possíveis vieses e limitações na pesquisa, foi utilizada a triangulação de métodos e fontes de dados. Essa abordagem metodológica envolve a utilização de múltiplas perspectivas, técnicas e informações para obter uma compreensão mais abrangente e confiável do objeto de estudo (Eisenhardt, 1989).

O trabalho foi estruturado em cinco fases fundamentais: 1) pesquisa exploratória, como investigação preliminar para entender o problema e identificar possíveis questões de pesquisa; 2) pesquisa bibliográfica, como etapa para levantamento das obras publicadas sobre o tema, como livros, artigos, teses, relatórios, entre outros; 3) revisão da literatura, na seleção e aprofundamento das principais teorias, conceitos, modelos e abordagens relacionados ao tema, bem como de iniciativas implementadas por governos e instituições para prevenir ou mitigar a guerra cognitiva nas redes sociais. Essa etapa também permitiu estabelecer a problemática e a

pergunta de pesquisa a partir de uma análise crítica do material selecionado; 4) estudo *ex-post facto* e análise comparativa, como abordagem complementar à revisão da literatura, para identificar as similaridades e diferenças do fenômeno em contextos específicos, praticados por atores estatais e privados, considerando sua complexidade e dinamismo; 5) pesquisa *survey*, para validar e aprofundar,, com especialistas a compreensão dos conceitos e modelos identificados e sua aplicação ao contexto brasileiro.

No capítulo 1, a introdução contextualiza a guerra cognitiva, destacando como este conflito impacta o domínio da mente humana por meio da manipulação de informações e emoções, representando uma ameaça à integridade da informação e à estabilidade social. Essa abordagem justifica a importância de se investigar esse desafio e entender como ele afeta a segurança do país e o funcionamento da democracia.

O capítulo 2 aprofunda o entendimento sobre a guerra cognitiva, concentrando-se nos principais elementos característicos do ambiente virtual das redes sociais. Isso inclui a curadoria algorítmica, o uso de inteligência artificial (IA), a disseminação de desinformação e *fake news*, as operações de influência digital, entre outros. Essa análise detalhada justifica a importância de entender os mecanismos subjacentes a essas ameaças que estão em ascensão.

No capítulo 3, a pesquisa apresenta uma análise comparativa a partir de um estudo *ex-post facto* de casos que abordam as táticas de guerra cognitiva online usadas pela Rússia e pela China, além das operações de manipulação da *Cambridge Analytica*. A importância de se compreender como esses atores disseminam a guerra cognitiva nas redes sociais justifica o exame dessas experiências. Identificar as diferenças e similaridades proporciona uma compreensão mais ampla das ameaças as quais o Poder Nacional brasileiro pode estar sujeito.

O capítulo 4 aborda como a guerra cognitiva afeta a maneira como o Poder Nacional se manifesta psicologicamente e socialmente, destacando a importância de proteger essa dimensão essencial do poder. A análise é importante para entender como a manipulação de informações nas redes sociais pode impactar a coesão social e a estabilidade política, evidenciando potenciais riscos para a segurança e integridade democrática nacional.

Os capítulos 5 e 6 tratam da metodologia e da análise dos dados da pesquisa, respectivamente. O capítulo 5 detalha os métodos adotados para garantir que a pesquisa fosse sólida e consistente. Os passos tomados para coletar, analisar e interpretar os dados de maneira organizada e segura são claramente explicados no capítulo. A análise dos dados da *Survey* no capítulo 6 revela descobertas importantes sobre as dinâmicas da guerra cognitiva e suas implicações para a Expressão Psicossocial do Poder Nacional.

O capítulo 7 apresenta as ações existentes utilizadas por diversas entidades nacionais e estrangeiras no enfrentamento das estratégias de manipulação da informação. Essas iniciativas oferecem uma base importante para formulação de políticas públicas de defesa nacional contra a guerra cognitiva nas redes sociais. Essa abordagem complementar se justifica necessidade de adotar procedimentos e iniciativas regulatórias que forneçam mecanismos de defesa da segurança nacional e da democracia.

O capítulo final deste trabalho busca, portanto, consolidar os achados da pesquisa e apresentá-los para que seja de significativa importância tanto para o desenvolvimento teórico quanto prático. O capítulo resume não apenas as principais descobertas, mas também indica a contribuição da pesquisa para o campo de estudo e novos caminhos de exploração.

2 DESAFIOS E DINÂMICAS EMERGENTES DA GUERRA COGNITIVA NAS REDES SOCIAIS

Quando o estrategista militar Carl von Clausewitz (1996) escreveu sobre o conceito de "névoa da guerra" no século XIX, ele não poderia antever as dificuldades exponenciais que os analistas militares enfrentariam para acessar informações precisas e manter uma compreensão clara da situação dos conflitos nos ambientes virtuais contemporâneos. O advento das redes sociais nas plataformas online gerou uma complexa teia de relações, onde a rápida disseminação de informações, a multiplicidade de fontes e a influência da desinformação contribuem para uma "névoa digital", em que o limite entre o fato verídico e o falsificado se torna cada vez mais tênue. Esse fenômeno superdimensionado destaca a relevância atemporal do conceito de Clausewitz nas novas conflitualidades, agora adaptado aos desafios modernos da guerra cognitiva, onde a incerteza e a falta de clareza online intensificam a complexidade das estratégias de manipulação e influência.

Transcendendo os campos de batalhas tradicionais, a guerra cognitiva busca influenciar a opinião pública e atingir objetivos estrategicamente planejados por meio da disseminação de desinformação e construção de narrativas cuidadosamente elaboradas, sendo um instrumento poderoso e, ao mesmo tempo, difícil de ser compreendido e superado. Enfrentar esse desafio requer do Estado brasileiro não apenas uma compreensão aprofundada das dinâmicas das redes sociais, mas também estratégias robustas para monitorar, prevenir e combater a manipulação cognitiva no ambiente digital (Claverie; Cluzel, 2022).

Segundo o relatório final da CPI de 8 de Janeiro (Congresso Nacional, 2023), o Brasil ocupa o terceiro lugar como o país que mais utiliza redes sociais globalmente, contando com mais de 131 milhões de contas ativas em diversas plataformas. Esses números demonstram o tamanho da influência das redes sociais na sociedade contemporânea e evidenciam os potenciais riscos significativos para a democracia com a disseminação de desinformação, a polarização política e a manipulação de opiniões públicas, em um cenário de guerra cognitiva. As redes sociais têm sido usadas tanto para fomentar conflitos quanto para revelar novos aspectos desses eventos.

Este capítulo procura empreender uma análise sobre essa complexa interseção entre a guerra cognitiva e as plataformas digitais, explorando definições fundamentais e conceitos dos diferentes tipos de guerra, como as guerras de informação, psicológica, cibernética e suas similaridades com a guerra cognitiva. Percorre as características peculiares da guerra cognitiva no ambiente online, examinando temas como polarização, extremismo e a influência dos

algoritmos na disseminação de conteúdos problemáticos e na criação de bolhas sociais. Em seguida, destaca os impactos significativos da guerra cognitiva nas redes sociais, desde a manipulação política até a disseminação de desinformação e *fake news*, incluindo uma análise da fragmentação do poder e suas implicações na segurança nacional e internacional. Os tópicos subsequentes exploram o tema específico das redes sociais como um novo teatro de operações, além da disseminação da infodemia, o conceito emergente de hiperinteligência, as operações de influência e retórica, e o recrutamento de extremistas por meio das redes sociais. Cada fragmento proporciona uma compreensão aprofundada e crítica, contribuindo para o entendimento abrangente dos desafios e dinâmicas enfrentados.

2.1 HEURÍSTICA CONCEITUAL

A guerra cognitiva é um conceito em evolução na literatura, associado ao rápido desenvolvimento de novas tecnologias e ao avanço do conhecimento sobre a cognição humana, bem como ao maior envolvimento da opinião pública nos conflitos contemporâneos. O tema tem sido objeto de debate e preocupação por parte de governos e instituições de Defesa. Bernal *et al*. (2020) sugerem que esse novo tipo de conflito moderno emergiu como uma estratégia para evitar confrontos diretos devastadores entre superpotências. Desta forma foram-se estabelecendo as guerras por procuração, nos quais as nações dominantes apoiavam ou se opunham a pequenos países ou grupos armados, criando um cenário de confronto indireto. Nesse contexto, agências como a *Central Intelligence Agency* (CIA), o *Federal Bureau of Investigation* (FBI) e o *Committee for State Security* (KGB) conduziram diversas operações de forma discreta. A partir dos anos 2000, observou-se um aumento significativo nas ações de desestabilização, marcando uma evolução na natureza e na intensidade da guerra cognitiva.

Na análise de conceitos complexos como os de guerra, utilizou-se heurísticas conceituais – ou seja, estratégias simplificadas e regras práticas – para entender melhor as relações entre eles (Russell; Norvig, 2010). Em busca de uma compreensão mais específica sobre o significado da guerra cognitiva nas redes sociais, realizou-se uma seleção criteriosa de alguns tipos de guerra, considerando sua relevância e impacto na formação da opinião pública, bem como seu efeito na segurança nacional e na integridade das democracias contemporâneas. Essa abordagem seletiva procurou proporcionar uma análise dos fenômenos envolvidos, realçando os aspectos que contribuem significativamente para as questões relacionadas à informação e à sua influência na percepção e compreensão de fatos e eventos diversos.

Como um componente essencial do espectro da guerra híbrida, a guerra cognitiva representa uma forma sofisticada de conflito que transcende os tradicionais campos de batalha físicos. Ao aproveitar as amplas oportunidades oferecidas pelas plataformas digitais, esta forma de guerra se insinua nas mentes e nas percepções das populações, moldando narrativas, distorcendo realidades e minando a coesão social. A guerra híbrida, por sua vez, se apresenta como um paradigma desafiador no panorama geopolítico do século XXI (Jopling, 2018). Essa complexa modalidade de conflito é caracterizada pela convergência de métodos convencionais e não convencionais, militares e não militares, permeando todas as esferas da sociedade, desde o âmbito político e econômico até o social, religioso e cultural. Essa tendência de utilização da guerra híbrida nos conflitos é uma perspectiva considerada pelos especialistas em segurança internacional (Korybko, 2018).

Para a Organização do Tratado do Atlântico Norte (OTAN), esse novo modelo de guerra se distingue de tudo o que já foi visto anteriormente. Mesmo incorporando aspectos da guerra híbrida, a extensão e o grau de impacto que apresenta o tornam muito mais ameaçador do que seus antecessores, sendo único em sua execução e propósito: "A guerra cognitiva busca fazer com que os inimigos se destruam de dentro para fora" (Bernal *et al*., 2020, p.3)[6]. Os autores destacam a complexidade e os riscos associados à disseminação rápida e massiva de informações nas redes sociais:

> Hoje nos deparamos com os problemas que vêm com a capacidade das redes sociais de transmitir informações para bilhões de pessoas dispostas em questão de minutos. Devemos nos defender contra algoritmos que possam identificar quem seria o mais suscetível ao material postado e quem está mais disposto a divulgá-lo. A capacidade atual de falsificar e manipular informações é sem precedentes, e os recentes avanços na inteligência artificial também tornaram o vídeo e o áudio suspeitos. [...] Em um mar de um bilhão de vozes, identificar fontes individuais tornou-se incrivelmente difícil (Bernal *et al*., 2020, pp. 3 e 4, tradução nossa)[7].

Três vertentes principais são consideradas relevantes neste estudo para compreender a complexidade e os impactos da guerra cognitiva: a guerra de informação, a guerra psicológica e a guerra cibernética. Essa seleção se sustenta pela interconexão que apresentam na dinâmica

---

[6] *"Cognitive warfare seeks to make enemies destroy themselves from the inside out".*

[7] *"Today we are faced with the problems that come with social media's ability to broadcast information to billions of willing people in a matter of minutes. We must defend against algorithms that can identify who would be the most susceptible to posted material, and who is most willing to spread it. The present-day ability to fake and manipulate information is unprecedented, and recent advancements in artificial intelligence have now made video and audio suspect as well. [...] In a sea of a billion voices, pinpointing individual sources has become incredibly difficult."*

global da influência, manipulação, disseminação e no uso estratégico de informações. Além desses componentes, são considerados também os desafios emergentes relacionados à privacidade dos dados pessoais, à segurança cibernética das infraestruturas críticas e às vulnerabilidades dos sistemas de inteligência artificial, que podem ser explorados para disseminar desinformação de maneira mais sofisticada e ampla. Cada uma delas apresenta características, objetivos e métodos específicos e que, muitas vezes, se confundem pela similaridade, desempenhando um papel distinto e ao mesmo tempo congruente nesse complexo ecossistema informacional. No entanto, é essencial reconhecer que, embora distintas, essas vertentes não operam de forma isolada, mas sim em sinergia, potencializando os efeitos umas das outras e ampliando a complexidade do contexto em que operam.

Para explicar as diferentes formas de guerra (informação, psicológica, cibernética e cognitiva) foi adotada a seguinte heurística conceitual: identificação dos conceitos-chave que definiam os diferentes tipos de guerra moderna, como controle de informação, manipulação psicológica, disrupção tecnológica e controle cognitivo; análise das estruturas conceituais subjacentes a cada modalidade; investigação das premissas implícitas sobre o papel da informação, psicologia, tecnologia e cognição; e exploração das metáforas e analogias para enquadrar e comunicar esses fenômenos complexos.

2.1.1 Guerra de Informação

A guerra de informação é uma estratégia que tem por objetivo o controle e manipulação das informações disponíveis para um público específico. Isso envolve a seleção deliberada de notícias, dados e narrativas para influenciar a percepção do público sobre eventos políticos, sociais ou militares. São utilizadas ações defensivas no espaço físico e virtual para proteger o acesso, processamento e comunicação de informações da força amiga, além de táticas ofensivas para negar, explorar, corromper ou destruir a capacidade de uma força adversária no uso das informações. As partes envolvidas na guerra de informação podem empregar táticas como propaganda, desinformação e censura para moldar a visão do público de acordo com seus objetivos. O foco está na gestão ativa da informação para obter vantagem estratégica (Murphy, 2022).

Bernal *et al*. (2020) explicam que a principal diferença entre a guerra de informação e a guerra cognitiva é que a primeira não diferencia as informações táticas do campo de batalha das informações destinadas ao público. Enquanto a guerra de informação procura o controle

absoluto da informação, a guerra cognitiva busca o controle de como os indivíduos e as populações reagem às informações recebidas.

2.1.2 Guerra Psicológica

A guerra psicológica se concentra na manipulação das emoções e sentimentos do público escolhido. Essa estratégia visa influenciar as atitudes e reações emocionais das pessoas, muitas vezes usando também táticas que envolvem propaganda, além de operações psicológicas (PsyOps) e manipulação de percepções para alcançar propósitos estratégicos. Nesse tipo de guerra, dedica-se a transmitir determinadas mensagens com o objetivo de criar uma resposta emocional específica, afetando psicologicamente o adversário, subvertendo sua moral, desencorajando-o ou desestabilizando-o (Lasswell, 1971; Coimbra, 2007).

Rodríguez (2020) explica que a guerra psicológica abrange diversas táticas de combate empregadas sem recorrer à força física, com o objetivo de influenciar valores, crenças, emoções, motivações, raciocínio ou comportamento de uma ou mais pessoas, nas esferas policial, militar ou política. Estas técnicas frequentemente são utilizadas para obter confissões ou fortalecer atitudes e comportamentos, por vezes sendo combinadas com operações de Guerra Não Convencional (GNC). O público-alvo pode incluir governos, organizações, grupos ou indivíduos.

2.1.3 Guerra Cibernética

A guerra cibernética representa uma forma de conflito que transcende fronteiras nacionais, podendo ser empregada tanto por estados soberanos quanto por atores não estatais e até mesmo por indivíduos. Sua natureza intrínseca envolve não apenas ataques diretos a sistemas de informação, mas também uma série de efeitos colaterais de natureza psicológica, econômica e política. O comprometimento de sistemas críticos de comunicação e a manipulação de dados podem levar a uma desestabilização psicológica em larga escala, minando a confiança nas instituições e nas próprias estruturas sociais. Além disso, a guerra cibernética não se restringe apenas ao âmbito psicológico, mas também possui consequências econômicas tangíveis com perdas financeiras substanciais para empresas e instituições governamentais alvo das operações (Greenberg, 2022).

Este tipo de guerra se refere à capacidade de interromper as infraestruturas tecnológicas e sistemas de comunicação de um país específico. A estratégia envolve ataques direcionados a

redes de computadores, sistemas de controle e outros ativos tecnológicos críticos. Os objetivos incluem a sabotagem de operações militares, a interrupção de serviços essenciais e a criação de desordem por meio de manipulação digital. No âmbito da guerra cognitiva, as ações procuram explorar vulnerabilidades tecnológicas para minar as capacidades de um adversário utilizando, por exemplo, práticas como *hacking* (invasão de sistemas para obtenção de informações), *pishing* (envio de mensagens fraudulentas), vazamento seletivo de informações, ataques sob bandeiras falsas *(false flag attacks)* para dificultar sua autoria, entre outros (Clarke; Knake, 2012).

No âmbito político, a guerra cibernética pode ser empregada como um instrumento para comprometer a soberania e a legitimidade de governos, manipulando dados para impactar eleições, desestabilizar sistemas e expandir as desigualdades sociais. A crescente dependência de infraestruturas digitais expõe os países a esse tipo de manipulação, ressaltando a urgência de estratégias sólidas de defesa e segurança cibernética (Rid, 2013).

2.1.4 Guerra Cognitiva

Mais sutil e sofisticada do que a guerra de informação, a guerra cognitiva (CogWar, na sigla em inglês) é uma forma de conflito que transcende os demais tipos de guerra citados, indo além da simples manipulação de dados ou emoções: "Os alvos desses ataques não são fábricas ou instalações militares, mas o próprio tecido de nossa sociedade, atingindo nossos *smartphones*, computadores e meios de comunicação" (Morris *et al*, 2024, tradução nossa)[8]. Os Estados Unidos da América (EUA) utilizam o termo "guerra cognitiva" desde 2017 para descrever a estratégia adotada por um Estado ou grupo de influência com o objetivo de "manipular um inimigo ou os mecanismos de cognição de seus cidadãos para enfraquecer, penetrá-lo, influenciá-lo ou mesmo subjugá-lo ou destruí-lo" (Underwood, 2017)[9].

Esse tipo de guerra engloba atividades coordenadas e executadas em conjunto com outros instrumentos de poder, como o militar, o econômico e o diplomático. A abordagem integrada é articulada para influenciar a percepção, as crenças e os comportamentos das populações-alvo, utilizando não apenas a informação estratégica, mas também a relativização da verdade, a desinformação, a propaganda e a manipulação psicológica como ferramentas

[8] *"The targets of these attacks are not factories or military installations but the very fabric of our society, reaching into our smartphones, computers, and media outlets".*

[9] *"manipulate an enemy or its citizenry's cognition mechanisms in order to weaken, penetrate, influence or even subjugate or destroy it".*

fundamentais. Seu objetivo é controlar como o público selecionado pensa e reage, criando uma situação mental favorável e exercendo influência na tomada de decisões (Bernal *et al*., 2020). Os objetivos podem ser conquistar um território, interromper os serviços públicos, provocar uma mudança de governo, influenciar eleições, minar a confiança, inibir o pensamento crítico ou desestabilizar e influenciar uma população, radicalizando a opinião, desacreditando os órgãos governamentais, desencadeando ou inibindo ações (Cluzel, 2020).

Diferentemente da guerra informacional, a guerra cognitiva busca alcançar resultados com efeitos potencialmente duradouros, independentemente da veracidade das informações divulgadas. Envolve influenciar a maneira como as pessoas percebem e interpretam informações, moldando o processo de aquisição, armazenamento, recuperação e uso cognitivo de informações. Utiliza ferramentas cibernéticas e tecnologia da informação para melhorar a personalização e a análise comportamental (Cluzel, 2020).

A guerra cognitiva integra capacidades cibernéticas, de informação, psicológicas e de engenharia social[10] em uma rede transnacional de fontes. Seu objetivo é criar confusão, desinformação e incerteza por meio de uma sobrecarga de informações. Essa estratégia concentra-se em alvos vulneráveis, introduz narrativas falsas, radicaliza indivíduos e amplifica a polarização social (Claverie *et al*., 2021).

Bucci, Cristofaro e Giardino (2023) reforçam o debate sobre o excesso informacional. Os autores explicam que a guerra cognitiva acontece em um ambiente saturado de informações. A rápida evolução das tecnologias digitais possibilita a disseminação instantânea e em massa de diversas narrativas contraditórias, muitas vezes sem a devida consideração sobre suas inconsistências, contradições ou falta de coerência, o que leva à sobrecarga informacional e à fadiga mental. Essa incapacidade de filtrar e classificar uma grande quantidade de informações deixa o indivíduo suscetível a mensagens persuasivas, o que contribui para o compartilhamento de notícias falsas, descontextualizadas ou tendenciosas.

A carga informacional excessiva está diretamente relacionada ao conceito da "economia da atenção", uma dinâmica que, segundo Lanham (2006), envolve a interação e os processos que definem como a atenção humana é gerenciada, capturada e valorizada, tornando-se um fenômeno central na era da informação digital. Neste novo paradigma, o tempo e a atenção dos usuários se tornaram recursos altamente disputados. Com a proliferação de conteúdo online,

[10] Os ataques de engenharia social são estratégias manipulativas online que levam os indivíduos a cometerem erros prejudiciais à sua segurança pessoal ou organizacional. Ao contrário de ataques que exploram vulnerabilidades técnicas, a engenharia social se baseia na manipulação psicológica e na exploração de falhas humanas, sendo às vezes denominada "*hacking* humano" (IBM, 2023b).

criadores e disseminadores de informação competem intensamente para capturar a atenção limitada do público. Esse excesso de informações digitais gera uma sobrecarga cognitiva, dificultando a reflexão aprofundada sobre os temas. Nesse contexto, as pessoas tendem a formar opiniões com base no impacto imediato das notícias, em vez de analisar cuidadosamente os fatos relacionados. Essa dinâmica pode levar a julgamentos superficiais e a uma compreensão fragmentada da realidade. A guerra cognitiva se aproveita desse ambiente de disputa pela atenção e sobrecarga informacional, prejudicando a capacidade das pessoas de processar as informações de maneira crítica. Essa dinâmica favorece a disseminação de narrativas distorcidas e a manipulação da opinião pública.

Complementando a análise de Lanham (2006), Castilho (2024) explica que, na guerra cognitiva da era digital, a busca por atenção e influência supera a preocupação com a veracidade da informação. O importante não é a qualidade da informação ou um conteúdo preciso, mas sim o impacto que ele gera. Nessa lógica, conceitos como verdade, exatidão e relevância cedem espaço para uma estratégia puramente competitiva, cujo único objetivo é conquistar a atenção e a adesão do público, amplificando o efeito da "viralização" de comentários e notícias, mesmo que sejam falsas. Com essa estratégia, procura gerar desconfiança ou resistência em relação a quaisquer informações que contrariem os interesses do grupo manipulador.

Essa dinâmica representa uma transformação preocupante nos padrões que deveriam orientar a circulação de informações. Os criadores de conteúdo podem recorrer a táticas questionáveis, como a divulgação de informações distorcidas ou mesmo falsas, desde que atendam ao propósito de atrair atenção e moldar a narrativa dominante. Essa guerra cognitiva tem implicações graves para a formação de opiniões e a tomada de decisões na sociedade, fomentando um ambiente de desinformação e polarização (Castilho, 2024). Uma vez que a cognição abrange todos os aspectos da função intelectual, incluindo elementos subconscientes e emocionais, que influenciam as decisões humanas, ao utilizar técnicas que vão além da simples divulgação de dados, a guerra cognitiva busca não apenas informar, mas manipular a maneira como as informações são compreendidas, interpretadas e internalizadas pelo público-alvo (Bernal *et al*., 2020).

O autor explica, ainda, que, além da exploração das vulnerabilidades psicológicas, cognitivas e emocionais do adversário, os métodos utilizados na guerra cognitiva também aproveitam as tendências e vieses cognitivos para moldar a percepção da realidade. Tudo isso é amplificado pelo uso de tecnologias como inteligência artificial e *big data*, além das redes sociais, que permitem uma difusão em larga escala e aumentam o impacto das ações.

Essas tecnologias permitem que os atores envolvidos nas operações monitorem e explorem as informações que circulam online, entendam padrões comportamentais e preferências dos alvos, e criem experiências que moldam a percepção da realidade. Isso permite uma manipulação mais eficaz da opinião pública e da tomada de decisão, tornando a guerra cognitiva uma ferramenta poderosa para influenciar a cognição e o comportamento dos adversários (Bernal *et al*., 2020).

A guerra cognitiva atua em diversas áreas visando influenciar a opinião pública, polarizar debates, deteriorar a confiança nas instituições, prejudicar a tomada de decisão estratégica, desmoralizar forças militares, criar pânico e promover a desinformação. Os atores envolvidos nesse tipo de conflito variam de Estados a organizações privadas. Essa característica assimétrica e multidimensional representa um desafio significativo para sua identificação e atribuição, além de exigir o desenvolvimento de competências individuais e sociais (Bernal *et al*., 2020).

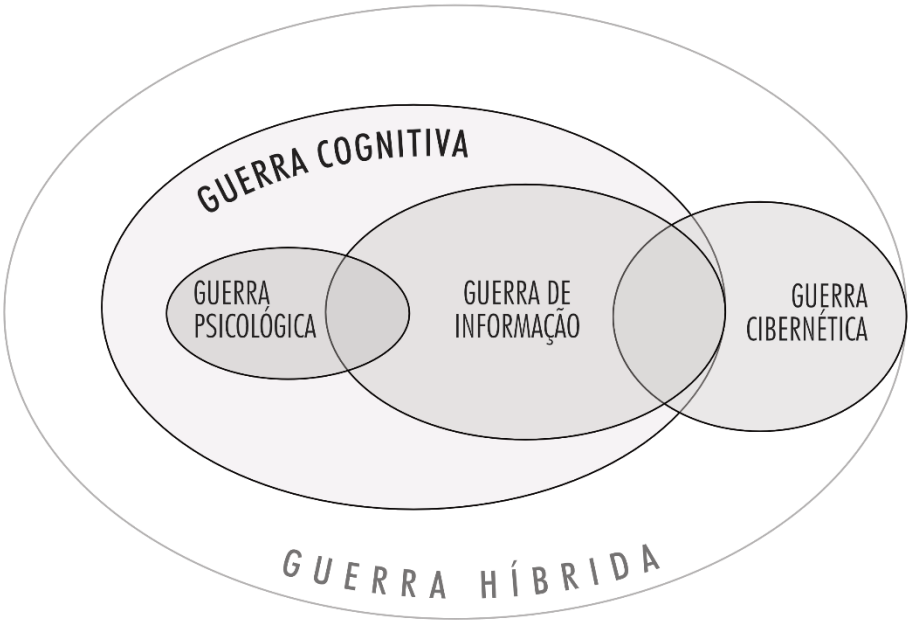
Tabela 1 – Comparação entre os tipos de guerra e a guerra cognitiva

Tipo de Guerra	Foco Principal	Métodos	Exemplos	Similaridades com a Guerra Cognitiva	Diferenças da Guerra Cognitiva
Informação	Controle e manipulação de informações	Propaganda, desinformação, censura, manipulação de dados	Campanhas de notícias falsas, campanhas de deslegitimação, interceptação de informação, alteração de informações	Manipulação de informações	Foco restrito à informação, sem influenciar a cognição
Psicológica	Manipulação de emoções e sentimentos	Propaganda, campanhas psicológicas, manipulação de percepções	Ataques à moral, incitação ao medo, condicionamento e persuasão	Influência emocional	Foco em emoções, sem controle da cognição
Cibernética	Interrupção de infraestruturas tecnológicas e sistemas de comunicação	Ataques de *hackers*, sabotagem, *pishing,* sequestro de dados	Ataques a infraestrutura de informação e sistemas de controle	Exploração de vulnerabilidades tecnológicas	Foco em tecnologia, sem manipulação de informações ou cognição
Cognitiva	Controle e manipulação do pensamento, comportamento e crenças	Criação de narrativas, agendas, uso de símbolos, promoção de ideologias, engajamento em comunidades online	Campanhas de desinformação, polarização social, erosão da confiança nas instituições	-	-

Fonte: Elaborado pela autora, com base em: Murphy (2022); Bernal *et al*. (2020); Lasswell (1971); Rodríguez (2020); Clarke e Knake (2012); Rid (2013); Greenberg (2022); Underwood (2017); Cluzel (2020); Castilho (2024); Bucci, Cristofaro e Giardino (2023); Claverie *et al* (2021) e Lanham (2006).

A relação conceitual entre guerra cognitiva e os outros três tipos de guerra pode ser compreendida através do elemento comum de influência e impacto na cognição humana, conforme verificado na Figura 1. No entanto, a guerra cognitiva se distingue por seu foco específico no controle dos processos cognitivos.

Figura 1 - Esquema conceitual entre os tipos de guerra



Fonte: Adaptado pela autora, baseado em Hung e Hung (2020).

2.2 MECANISMOS DA GUERRA COGNITIVA NO AMBIENTE VIRTUAL

As redes sociais têm conquistado relevância significativa na sociedade contemporânea, transformando a forma como as pessoas se comunicam, consomem informações, interagem e participam da esfera pública. Este fenômeno é impulsionado pela rápida evolução da tecnologia digital e pela disseminação da conectividade online. Interfaces amigáveis, recursos multimídia e ferramentas interativas facilitam a navegação e a criação de conteúdo, popularizando o acesso à comunicação online (Jenkins; Ford; Green, 2013).

Plataformas virtuais como Facebook, X (antigo Twitter), Telegram, Instagram e LinkedIn, por exemplo, têm se tornado espaços predominantes e indispensáveis para a interação social global, permitindo que indivíduos se conectem instantaneamente, transcendendo fronteiras geográficas e culturais. Esses aplicativos não apenas facilitam a comunicação entre

amigos e familiares, mas também desempenham um papel fundamental na formação de comunidades virtuais baseadas em interesses comuns, criando um ambiente dinâmico de troca de ideias e desempenhando uma função central na disseminação de informações e na influência de opiniões (Han, 2022).

Nesse novo contexto, a geopolítica do século XXI, marcada por uma profunda transformação, testemunha a ascensão de novos polos de poder que desafiam a hegemonia unipolar que entrou em vigor com o fim da Guerra Fria (1947-1991). O teatro de operações ganhou novas fronteiras, se expandindo para o domínio cognitivo e para as plataformas de rede social, tornando as decisões domésticas com potencial para gerar impactos internacionais e as questões de política externa com implicações no âmbito nacional. Essa mudança exige repensar os conceitos e estratégias de segurança e Defesa, levando em consideração as complexas interações entre os diversos atores internacionais, potencializadas pela comunicação online (Wilson III; Smitson, 2020).

Um estudo encomendado pela OTAN ao contra-almirante Cluzel (2020) propõe a guerra cognitiva como um novo domínio operacional e a identifica como uma terceira dimensão do campo de batalha: "Às dimensões física e informacional é agora adicionada uma dimensão cognitiva. Esta última cria, assim, um novo espaço de competição, para além dos domínios terrestre, marítimo, aéreo, cibernético e espacial" (Cluzel, 2020, p.1, tradução nossa)[11]. A análise também reconhece as redes sociais como uma arena fundamental dessa nova realidade, utilizada para a disseminação de desinformação, propaganda e influência psicológica em massa. A explosão de dados comportamentais, segundo Cluzel, tem permitido avanços significativos na compreensão das dinâmicas de indivíduos e grandes grupos online. À medida que esse campo de pesquisa se expande, surgem inúmeras oportunidades para utilizar esse conhecimento na criação de técnicas poderosas, não apenas para compreender, mas também para influenciar o comportamento e as crenças das pessoas, tanto em nível individual quanto global (Cluzel, 2020).

Considerada como uma nova modalidade de guerra, a guerra cognitiva envolve estratégias mais profundas, como a criação de narrativas específicas, o estabelecimento de agendas, o uso de símbolos e a promoção de ideologias que sirvam aos objetivos da parte disseminadora. Essa forma de guerra tem seu foco central no controle da cognição, buscando moldar as percepções e interpretações das informações pelo adversário. Ela vai além da abordagem tradicional centrada na derrota do oponente, expandindo o escopo e os objetivos do

[11] *"To the physical and informational dimensions is now added a cognitive dimension. The latter thus creates a new space of competition, beyond the land, maritime, air, cybernetic and spatial domains."*

conflito. “O princípio mais importante não é apenas seguir uma estratégia e vencer sem lutar [...], é também uma guerra contra o que um alvo adversário pensa, gosta ou acredita, modificando suas representações da realidade” (Cluzel, 2020, p. 3, tradução nossa)[12].

Nas redes sociais, essas estratégias encontram um terreno fértil, onde a criação de bolhas informativas ou *clusters* pode limitar a diversidade de ideias e a compreensão de diferentes perspectivas (Santaella, 2018; Pariser, 2011). Como resultado, tópicos relevantes e eventos atuais se espalham rapidamente por meio de compartilhamentos, “curtidas” e comentários, contribuindo para a radicalização de ideias sobre diversas questões, como sociais, políticas e religiosas, entre outras. Além disso, uma preocupação que se torna cada vez mais desafiadora para governos e autoridades é o poder de disseminação das *fake news* (notícias falsas) e da desinformação.

Allcott *et al* (2019) reforçam o argumento de que as bolhas de filtro e os algoritmos das redes sociais que priorizam o engajamento representam uma ameaça à integridade da informação e à sociedade em geral. Esse ambiente, altamente personalizado, possibilita que os conteúdos polarizadores alcancem vastas audiências em intervalos de tempo reduzidos. A manipulação da percepção, a amplificação das divisões sociais e a falta de clareza sobre a veracidade das informações culminam em uma espécie de dissonância cognitiva, tornando essas características, essenciais desse fenômeno, em um instrumento poderoso e, simultaneamente, desafiador de ser compreendido e confrontado.

Axel Bruns, em seu livro *Are Filter Bubbles Real?* (2019), contrapõe a ideia, questionando se a preocupação com as bolhas de filtro e câmaras de eco *(eco chambers)* online se justifica. Ele considera essa visão um exagero e pondera que, na realidade, esse debate é uma tentativa de desviar a atenção de questões mais sérias, como a hiperpolarização e a ascensão do populismo nas democracias. Bruns destaca que os usuários não são apenas passivos diante dos algoritmos, mas há um papel ativo na seleção do conteúdo que consomem. Esses mecanismos não criariam bolhas isoladas, ao contrário, poderiam, na verdade, expor os usuários a uma gama mais diversa de conteúdo.

A utilização das redes sociais como o novo campo de batalha da guerra cognitiva representa um desafio significativo, exigindo não apenas profundo entendimento desses ambientes, mas também de estratégias robustas para monitorar, combater e prevenir essa insidiosa ameaça para a democracia e a estabilidade social. Com o propósito de oferecer uma visão abrangente e auxiliar na compreensão das complexas camadas desse novo tipo de conflito,

[12] “*The main principle is not only to follow a strategy and win without fighting (a principle dear to Sun Tzu), it is also a war against what an opposing target thinks, likes or believes by modifying its representations of reality”.*

apresenta-se a seguir uma abordagem que considera a interdisciplinaridade e a complexidade dos mecanismos, das dinâmicas e dos efeitos envolvidos nesse novo ambiente.

2.2.1 Curadoria algorítmica e bolhas de filtro

Algoritmos são estruturas de linguagem computacional desenvolvidas para atender a determinadas finalidades. Essas estruturas são frequentemente utilizadas por sistemas e plataformas digitais para personalizar a experiência do usuário ao melhorar buscas, analisar dados, segmentar audiências, identificar fraudes, traduzir automaticamente textos, processar imagens e vídeos e aplicar métodos de aprendizado de máquina em diferentes atividades. Um exemplo clássico é o *EdgeRank*, um algoritmo desenvolvido de forma pioneira pelo Facebook para otimizar e tornar o *feed* de notícias mais relevante, assegurando que os usuários tivessem acesso ao conteúdo de seu interesse e mantendo-os envolvidos e engajados por mais tempo na plataforma (Pariser, 2011).

Neste sentido, a curadoria algorítmica organiza e faz a manutenção da extensa base de dados dessas plataformas determinando quais conteúdos são exibidos com base nos interesses e comportamentos dos internautas – além de outras variáveis –, influenciando as escolhas e interações online. Esse processo, conhecido como fenômeno das "bolhas de filtro", tem impacto significativo na forma como as pessoas acessam e consomem informações na era digital, moldando suas experiências e perspectivas com base em recomendações e classificação de conteúdo (Corrêa; Bertocchi, 2012). Seaver (2019) destaca, entretanto, que os algoritmos são resultado de escolhas humanas e institucionais e não apenas objetos técnicos autônomos e neutros. Eles refletem as intenções dos desenvolvedores carregando um conjunto de ideias e decisões traduzidas em código.

Orlowski (2020), em seu documentário "O Dilema das Redes", destaca como os algoritmos são utilizados pelas redes sociais e empresas de tecnologia para manipular o comportamento dos internautas. Como editores invisíveis, esses algoritmos, embora muitas vezes percebidos como neutros, refletem os interesses e vieses dos programadores, podendo influenciar significativamente a exposição dos usuários a diferentes perspectivas.

Segundo o diretor (Orlowski, 2020), esse conjunto de instruções digitais bem definidas e ordenadas é uma ferramenta poderosa utilizada para coletar dados pessoais e customizar conteúdos, anúncios e recomendações, criando assim um ambiente propício para a disseminação de desinformação e polarização. Desta forma, os algoritmos das redes sociais são projetados para incentivar o usuário a permanecer conectado, transformando esse engajamento

em um modelo de negócio lucrativo para as empresas de tecnologia e em uma multidão de seguidores das mais variadas ideologias.

Assim como Allcott *et al* (2019), Orlowski (2020) explica que, na prática, os algoritmos tendem a promover o acesso a conteúdos problemáticos. Caso um usuário demonstre interesse em acessar vídeos relacionados a teorias de conspiração ou notícias falsas, os algoritmos são projetados para recomendar continuamente conteúdos semelhantes, visando atender às preferências do internauta. Esse processo contribui para a formação das bolhas sociais, intensificando a divisão social, o extremismo e a polarização da sociedade. Além disso, tal mecanismo cria ambientes propícios para que sistemas de inteligência artificial auxiliem na disseminação de notícias falsas e teorias conspiratórias, facilitando, desse modo, a manipulação política.

Ex-funcionários e executivos de empresas como Google, Facebook e X (antigo Twitter) que participam do documentário abordam diversos aspectos preocupantes relacionados ao impacto das redes sociais na sociedade. Eles alertam sobre a coleta massiva de dados pessoais pelas plataformas, a manipulação dos algoritmos e a influência sobre as decisões dos usuários. Também ressaltam a falta de transparência nessas práticas e defendem a necessidade urgente de regulamentação para proteger a privacidade e a integridade dos indivíduos online (Orlowski, 2020).

Segundo Sánchez e Ruiz (2019), o algoritmo de aprendizado de máquina *(machine learning)* analisa a "biblioteca de *fake news",* que se refere a uma coleção de conteúdos falsos já publicados, e identifica padrões na forma como os textos e imagens são combinados. Com base nesses padrões, o algoritmo é capaz de gerar novas combinações de textos e imagens que simulam a linguagem jornalística e aparentam ser informações neutras. Esse conteúdo é disseminado na internet e redes sociais. Essa biblioteca varia geralmente entre 10 mil e 50 mil peças, e serve como ponto de partida para a criação de novas *fake news*. Os autores explicam, ainda, que as redes sociais operam com um bem intangível, que são os dados dos usuários, e utilizam esses dados para criarem a inteligência artificial por meio das técnicas de *machine learning*: "Os usuários constroem IA sem saber, fornecendo o conteúdo que forma a base e o volume de atividade: sem acesso aos dados do celular, não haveria IA" (p. 60, tradução nossa)[13].

Cathy O´Neil, em "Algoritmos de destruição em massa" (2020), explora como esses algoritmos, muitas vezes obscuros e com ciclos viciados de *feedback*, podem perpetuar injustiças em diversos aspectos da vida, como educação, consumo, economia, saúde, segurança

[13] *"Los usuarios construyen sin saberlo la IA proporcio nando el contenido que constituye la base y el volumen de actividad: sin acceso a los datos de los teléfonos móviles, no habría IA".*

pública e vida cívica. Ela destaca que esses modelos matemáticos podem influenciar negativamente a democracia, o combate ao crime, as finanças, o trabalho e a aprendizagem, gerando consequências prejudiciais para a sociedade. A autora também defende a regulamentação desses algoritmos para evitar discriminações e garantir que sejam controlados e alinhados com os valores fundamentais da humanidade, pois podem refletir preconceitos, reforçar desigualdades e comprometer a privacidade individual.

Em contrapartida, estudos indicam que a seleção da amostra de dados é tão determinante para o resultado quanto o próprio algoritmo utilizado. No documentário *"Coded Bias"* (Kantayya, 2022), a pesquisadora do *Massachusetts Institute of Technology (MIT)*, Joy Buolamwini, aborda as falhas nos algoritmos de reconhecimento facial utilizados por grandes empresas de tecnologia como IBM, Microsoft, Google e Amazon. Ela descobriu que esses sistemas não conseguiam identificar corretamente rostos de pessoas negras. Esse não seria um problema do algoritmo em si, mas sim da amostra de dados utilizada para treiná-lo, que pode refletir vieses, ideais, crenças e experiências dos desenvolvedores. Neste caso, os conjuntos de dados selecionados para treinar esses algoritmos não representavam a diversidade populacional, sendo predominantemente compostos por rostos de pessoas brancas. Buolamwini demonstra que essa falta de diversidade nos dados de treinamento levou os algoritmos a aprender e reproduzir os preconceitos presentes na amostra, resultando em erros sistemáticos e discriminatórios.

2.2.2 Inteligência Artificial e automatização da guerra cognitiva

Os avanços tecnológicos exponenciais têm transformado profundamente o modo de interação e comunicação nas redes sociais. Com o crescimento da inteligência artificial (IA), análise de *big data* e algoritmos sofisticados, as plataformas digitais alcançaram capacidade sem precedentes de coletar, processar e utilizar dados. Essas habilidades podem ser aplicadas para melhorar a personalização e eficiência das interações online tanto quanto para influenciar o comportamento humano (Morais; Branco, 2022).

A inteligência artificial é um campo multidisciplinar da ciência da computação voltado para sistemas e tecnologias capazes de exibir comportamentos e habilidades inteligentes similares às humanas. Essas características incluem aprender, tomar decisões, resolver problemas, compreender linguagem natural e reconhecer padrões, entre outras infinitas possibilidades. A IA pode ser classificada em várias categorias, entre as quais se destacam a IA generativa (GenAI) e a IA preditiva, que servem a propósitos distintos. A IA generativa

emprega aprendizado de máquina *(machine learning)* para produzir novos conteúdos, como texto, imagens e áudio, com o uso de algoritmos treinados em grandes conjuntos de dados. A IA preditiva, por outro lado, antecipa comportamentos e resultados com base em informações passadas e presentes, identificando probabilidades e tendências (Miikkulainen, 2023; Emmert-Streib *et al*, 2020). Ambas podem ser utilizadas na disseminação da desinformação, criando conteúdos falsos que parecem autênticos, além de influenciar públicos específicos com informações direcionadas. Devido a essas possibilidades, a IA está sendo aplicada em conversas online e interações em redes sociais. Isso demonstra uma versatilidade e capacidade de influenciar as opiniões e comportamentos dos usuários, usando dados sobre seus interesses e hábitos, e se tornando cada vez mais sofisticada na forma como se comunica e interage (Brundage, 2018).

Com base nesse contexto virtual complexo e desafiador, Nick Bostrom (2018) postula que, neste século, ainda poderemos desenvolver a primeira inteligência artificial geral (IAG), que seria equivalente ou superior à inteligência humana. Essa tecnologia extremamente avançada poderá realizar qualquer tarefa cognitiva que um ser humano possa fazer. Ele destaca a importância de antecipar os impactos dessa evolução tecnológica, enfatizando a necessidade de se desenvolver mecanismos de controle para a superinteligência artificial antes da criação desses sistemas inteligentes, para garantir que sejam geridos de maneira segura e benéfica para a sociedade.

Um dos recursos mais poderosos da IA nas redes sociais é sua capacidade de processar grandes quantidades de dados do usuário, incluindo comportamentos, preferências e interesses. Quando combinado com sistemas superinteligentes, esse poder de análise pode tornar muito difícil – ou mesmo impossível – combater táticas de manipulação que visam influenciar a opinião pública. Isso pode levar à disseminação de desinformação e influência sobre decisões políticas, sociais e econômicas (Bostrom, 2018).

As plataformas de redes sociais que utilizam inteligência artificial (IA) em larga escala proporcionam um meio pelo qual indivíduos mal-intencionados podem disseminar informações enganosas ou conduzir campanhas de desinformação de forma rápida e extensa, sem uma constante supervisão humana. A introdução da IA generativa e conversacional adiciona complexidade a esse panorama. Estas tecnologias são notavelmente influenciadas pela arquitetura *Transformer*, introduzida pelo artigo *"Attention Is All You Need",* de Vaswani *et al.,* em 2017. Este modelo revolucionário promoveu avanços substanciais no campo da inteligência artificial, especialmente no processamento de linguagem natural. Ele se baseia em um sistema de "autoatenção" *(ou self-attention)* que consegue interpretar e ajustar cada palavra

dentro de uma frase de forma simultânea, analisando a importância relativa entre elas. Uma das vantagens do *Transformer* é a sua capacidade de processar palavras de maneira não linear, o que aumenta drasticamente a eficácia em tarefas como tradução automática e geração de texto.

A inteligência artificial generativa tem capacidade de criar novos conteúdos, seja em forma de textos, imagens, vozes simuladas ou até composições musicais. Isso tudo a partir de grandes conjuntos de dados já existentes. Por outro lado, a inteligência artificial conversacional visa facilitar a interação direta entre humanos e computadores, através de conversas em linguagem natural. O avanço dessas tecnologias se dá, principalmente, por meio de áreas como aprendizado de máquina (ML), processamento de linguagem natural (NLP), visão computacional (CV), redes neurais artificiais (ANNs) e análise preditiva (PA). Tais ferramentas são essenciais para desenvolver aplicações que automatizam e otimizam processos em diversos setores da indústria e serviços (Morais; Branco, 2022).

Esses grandes modelos de linguagem, *chatbots* poderosos, geradores de imagens e de vídeos, e softwares de simulação de voz, permitem a criação rápida de conteúdos complexos, de alta qualidade e potencialmente preocupantes. Quando essas capacidades de mídia sintética (criada ou modificada com o auxílio da inteligência artificial) são automatizadas, elas podem aumentar significativamente a geração e a disseminação de campanhas de desinformação, bem como apresentar "realidades" manipuladas em escala global. Isso é especialmente crítico no contexto político, onde a desinformação pode ter consequências graves para a democracia e para as decisões baseadas em dados (G7, 2022).

Sánchez e Ruiz (2019) destacam que a personalização de informações impulsionada pela inteligência artificial e pelas redes sociais resultou na criação de uma "economia da desinformação", em que a produção e disseminação de informações falsas fazem parte de um sistema econômico que recompensa monetariamente a propagação de conteúdo enganoso. Quanto mais polêmica a informação, maior é a chance de ser compartilhada e gerar receita para os disseminadores, por meio de cliques, visualização e engajamento. Nesse contexto, a produção informacional é adaptada às preferências do usuário, com um direcionamento específico do consumo de informações.

Esse fenômeno reflete a maneira como as plataformas algorítmicas utilizam dados dos usuários para personalizar ofertas comerciais e conteúdos. A disseminação de desinformação é favorecida nesse caso ao adaptar as informações de acordo com as preferências individuais. Essa prática pode levar às "bolhas sociais", reforçando crenças pré-existentes e limitando a exposição a visões divergentes, com prejuízo do senso crítico e da liberdade de escolha (Sánchez; Ruiz 2019).

Segundo Balbino (2022), os algoritmos de IA se adaptam e evoluem ao longo do tempo, ajustando suas estratégias com base nas informações recebidas e nas mudanças das condições do ambiente online. Desta forma, tornam-se mais resilientes a contramedidas e mais difíceis de serem detectados e neutralizados. Essas propriedades amplificam as estratégias da guerra cognitiva, tornando-as ainda mais eficazes na manipulação das mentes e na influência comportamental por meio das redes sociais, com "viralização" rápida e massiva de informações, disseminação de notícias falsas, criação de narrativas enviesadas e segmentação precisa de mensagens.

Além disso, os robôs de IA, também conhecidos como *bots*, exercem um papel relevante nas redes sociais. Ao serem projetados com a finalidade de interagir com os usuários de forma automatizada, emulando comportamentos humanos, tais programas são utilizados para uma gama variada de finalidades, que vão além da automação de tarefas simples, como responder a mensagens de correio ou fazer postagem programadas, a disseminação de desinformação. Eles também são utilizados para incrementar artificialmente o engajamento em determinados perfis ou páginas, criando uma ilusão de popularidade ou relevância. Isso é feito por meio de curtidas, compartilhamentos, comentários automáticos e outras interações simuladas, para manipular os algoritmos de recomendação e aumentar a visibilidade de conteúdos específicos (Ridolfo; Hart-Davidson, 2019).

Conforme apontam Sánchez e Ruiz (2019, p. 59, tradução nossa)[14], a economia da desinformação aproveita as inúmeras possiblidades da inteligência artificial e da automação "para criar um catálogo atualizado de conteúdos imprecisos". Eles acrescentam que a velocidade com que esse conteúdo é distribuído "dificulta a intervenção que tenha como propósito impedir a disseminação de mentiras" (p.59, tradução nossa)[15].

As *deepfakes*, um subcampo da *machine learning*, geradas a partir dos avanços da IA por meio de algoritmos de aprendizado profundo *(deep learning)*, representam da mesma forma desafios no ambiente digital. Esses recursos audiovisuais manipulados digitalmente apresentam conteúdo falso, porém com aspecto altamente realista. Essa tecnologia sofisticada permite modificar a aparência, a voz e outros atributos dos seres humanos para criar representações falsas e convincentes (Walter; 2022). O emprego dessa técnica se expande gradualmente à medida que a capacidade computacional evolui, conquistando atenção e interesse de usuários com perfis e objetivos diversos.

---

[14] *"para la creación de un catálogo actualizado de contenidos imprecisos".*
[15] *"dificulta la intervención para atajar la difusión de mentiras".*

Skove (2024) explica que o Exército dos Estados Unidos está utilizando as *deepfakes* para treinamento relacionado à guerra de informação. Um instrutor de operações psicológicas criou um programa de clonagem de voz, chamado *Ghost Machine*, utilizando apenas uma amostra de áudio e um computador. O programa replica padrões de respiração e pausas, imitando perfeitamente a voz de qualquer pessoa. A ideia do programa não é nova, mas demonstra o fácil acesso e o uso cada vez mais simples da técnica e de seu potencial na guerra cognitiva. Programas como o *Ghost Machine* podem ser utilizados para diversas finalidades, inclusive imitar vozes de autoridades e líderes com o intuito de desinformar, confundir os oponentes ou levá-los para armadilhas. Podem, também, transmitir informações falsas ou propaganda intencional, e até mesmo atacar o moral do inimigo, incentivando a deserção ou o abandono de posições, e espalhando desinformação sobre derrotas ou perdas para semear o desespero entre as tropas inimigas.

Outro desafio relacionado ao uso da inteligência artificial são os algoritmos neuromórficos, que podem imitar o funcionamento do cérebro humano e facilitar o desenvolvimento de sistemas mais eficientes e poderosos. Esses algoritmos são projetados para operar em hardware especializado. Eles são inspirados na estrutura e funcionamento dos neurônios e sinapses do cérebro, o que os torna mais eficazes em tarefas complexas de processamento de informações (Syed *et al*., 2023). A capacidade desses algoritmos de processar dados como o cérebro humano faz pode torná-los mais eficientes na criação de conteúdo persuasivo pela IA generativa modificando dados originais. Também podem identificar as vulnerabilidades psicológicas dos usuários, aumentando o potencial de resultados nas campanhas de desinformação e manipulação.

O uso desses algoritmos pela IA preditiva também pode intensificar as estratégias de manipulação e desinformação, tornando essas ameaças mais difíceis de combater. Um exemplo seria a aplicação de dados para prever quais notícias terão maior impacto e, com base nessas previsões, criar conteúdo para influenciar a opinião pública (Valadares, 2021).

2.2.3 Infodemia, desinformação e *fake news*

O termo “infodemia” foi cunhado pela primeira vez pelo analista de política externa, segurança nacional e assuntos políticos estadunidense, David J. Rothkopf, em 2003, em uma coluna no jornal *Washington Post*. No artigo, Rothkopf compara a quantidade exponencial de informação disponível à epidemia da Síndrome Respiratória Aguda Grave (SARS, na sigla em inglês), afirmando hiperbolicamente que a infodemia pode ser mais perigosa que o próprio vírus

respiratório. Essa epidemia de informações está cada vez mais frequente e se apresenta como uma das mais "virulentas" na sociedade contemporânea, capaz de afetar as economias nacionais e internacionais, a política e até a segurança de maneiras totalmente desproporcionais à realidade. Ele destaca que essas informações muitas vezes são misturadas com medo, especulação e boatos, sendo propagadas de maneira rápida e abrangente pelas redes sociais, amplificando seus efeitos (Rothkopf, 2003).

Em 1970, Alvin Toffler já antecipava os resultados dessa infodemia com a criação do termo "sobrecarga de informações" (*information overload*) para descrever quando indivíduos ou grupos de pessoas são inundados com informações acima de sua capacidade de processamento e assimilação. Segundo esse conceito, a hiperconectividade pode causar uma sobrecarga cognitiva ao expor o indivíduo a muitas informações sobre um determinado tema. O efeito seria a dificuldade ou impossibilidade de os indivíduos tomarem boas decisões em momentos decisivos (Toffler, 1970; Edmunds; Morris, 2000).

Essa intensificação do fluxo informacional possibilitou o surgimento e proliferação em larga escala da desinformação e das *fake news*. Esses dois termos são frequentemente confundidos pois se sobrepõem, mas há diferenças. Enquanto a desinformação se refere a qualquer tipo de informação enganosa, as *fake news* são um subtipo de desinformação que imita o padrão jornalístico para parecerem mais convincentes e ganhar credibilidade. Em muitos casos, essas informações pseudojornalísticas são disseminadas com o objetivo de criar uma desordem informacional, manipulando a opinião pública e gerando impactos negativos na sociedade, de acordo com Zimdars e Mcleod (2020). Os autores destacam que as *fake news* expõem problemas mais amplos, como a politização e o armamento da informação, a crise da mídia tradicional e a incapacidade tecnológica de controlar a disseminação de notícias falsificadas.

Segundo revelado pelo relatório final da Comissão Parlamentar de Inquérito (CPI) instaurada pelo Congresso Nacional brasileiro (2023) para investigar os atos antidemocráticos de 8 de Janeiro de 2023, um estudo do *Massachusetts Institute of Technology (MIT)*, publicado por Vosoughi *et al*. em 2018, constatou que as *fake news* se espalham significativamente mais rápido, com maior intensidade e de forma mais ampla do que notícias verdadeiras nas redes sociais. Estima-se que cerca de 70% dessas falsas notícias sejam compartilhadas com mais frequência do que histórias verídicas, conforme apontado pelos congressistas. Moulas e Boateng (2021) destacam uma constatação de uma pesquisa da *Johns Hopkins University*, que mostrou que uma postagem falsa pode dobrar seu alcance a cada 15 minutos, atingindo 16 milhões de pessoas em aproximadamente seis horas. A propagação mais fácil das informações

falsas pode ser atribuída a vários fatores, incluindo o apelo emocional que frequentemente acompanha essas histórias fabricadas, bem como o impulso para compartilhar, gerado pela surpresa, indignação ou o medo que elas podem provocar.

Para Haiden e Althius (2018), as campanhas de disseminação de *fake news* possuem quatro objetivos estratégicos principais. Primeiramente, algumas dessas notícias são disseminadas principalmente por interesses comerciais. Utilizando táticas sensacionalistas como os *"click baits"* (iscas de cliques), essas mensagens visam gerar receita por meio de publicidade, visualizações de página ou compartilhamentos nas redes sociais. No entanto, o conteúdo é enganoso e pode ser decepcionante ou até mesmo irrelevante em relação ao título chamativo que provocou o clique inicial.

Em segundo lugar, a desinformação pode ser usada para obter vantagens políticas. Um exemplo dessa prática é a falsa acusação de exploração infantil que teria sido imputada ao gerente de campanha da candidata à presidência dos Estados Unidos, Hillary Clinton, e ao seu marido e ex-presidente dos EUA, Bill Clinton. Este caso foi amplamente explorado devido à associação indevida de ambos com a operação de uma suposta rede criminosa que, segundo alegações posteriormente consideradas infundadas, operaria em uma pizzaria em Washington, na capital estadunidense. Além disso, as estratégias mencionadas possuíam um viés político e não se limitavam a difamar o adversário. Elas incluíam táticas para limitar certos grupos sociais ao excluir comentários e conteúdo que não atendessem aos interesses próprios. Também utilizavam "*bots* sociais" (perfis automatizados) para disseminar informações. Essas abordagens são consideradas como essenciais para o sucesso de políticos populistas, pois manipulam a percepção pública e ampliam o impacto de mensagens estratégicas (Haiden; Althuis, 2018).

A desinformação pode ser uma ferramenta poderosa para desestabilizar a sociedade, fomentando a divisão entre diferentes grupos. Haiden e Althuis (2018) apontam que quem espalha esse tipo de conteúdo muitas vezes explora a ansiedade coletiva para minar a confiança nas instituições e criar um clima de desconfiança generalizada. Isso acaba amplificando conflitos, dividindo a sociedade de maneira profunda. A intenção é romper com qualquer sensação de tranquilidade, gerando um estado constante de incerteza e instabilidade, independentemente de qual seja o contexto social.

Por fim, a desinformação pode criar um clima de desorientação e confusão que acaba alimentando a si mesmo. Quando as pessoas são bombardeadas com informações conflitantes ou enganosas, elas começam a duvidar da realidade dos fatos, ficando cada vez mais confusas e céticas. Esse estado de desorientação se reforça, e muitos acabam buscando fontes alternativas

de informação, que muitas vezes são menos confiáveis ou até extremas. Nesse ponto, passa a ser difícil distinguir o que é verdade do que é falso (Haiden; Althuis, 2018).

O aumento das *fake news* nas redes sociais levou não apenas ao debate sobre a disseminação e os efeitos da desinformação, mas também à reflexão e discussão sobre o próprio conceito desse fenômeno. Segundo Barreto Junior:

> *Fake news* não são meras mentiras, mas sim uma sofisticada estratégia de comunicação política, que extrapola o marco temporal dos períodos eleitorais e instaura um ambiente de guerra permanente, que satura a agenda política e provoca efeitos deletérios na qualidade do debate público (2022, p. 5).

O autor reconhece que as *fake news* não se restringem atualmente às questões eleitorais, mas afetam amplamente o debate público diversificado, por meio das redes sociais, aplicativos de compartilhamento de mensagens e plataformas de vídeo. O termo cientificamente correto seria "Desinformação Adversarial, Táticas e Técnicas de Influência" (DATTI), mas passou a ser conhecido popularmente como *fake news.* O DATTI (do inglês *AMIT - Adversarial Misinformation and Influence Tactics and Techniques)* é usado por especialistas e pesquisadores para descrever o fenômeno da desinformação coordenada e da manipulação de informações. Nesse ambiente, para que a desinformação alcance eficácia, ela passa por uma "cadeia invisível e descentralizada de comandos" que possuem domínio amplo e proeminente do ambiente digital (Barreto Junior, 2022, p. 10).

Bucci (2022) explica que as *fake news* imitam o estilo e estrutura da notícia jornalística, mas na realidade são uma falsificação, uma distorção do verdadeiro padrão do jornalismo. As *fake news* subvertem o jornalismo legítimo, usando sua aparência para disfarçar intenções enganosas e prejudiciais. Blanco *et al* (2021) defendem que o vocábulo traz uma contradição, já que o princípio da notícia é divulgar algo verdadeiro, sendo as *fake news* uma informação enganosa. Alcott e Gentzkow (2017, p. 4, tradução nossa)[16], por sua vez, definem o termo como "artigos noticiosos que são intencionalmente e verificadamente falsos e que podem enganar os leitores". Há plataformas que mesclam notícias factuais com artigos falsos para gerar dissonância cognitiva e rapidamente se espalhar pelas redes sociais.

Sob o ponto de vista jurídico, Rais (2018) defende que, para ser considerada *fake news,* a informação enganosa não pode ser decorrente de um "simples erro" pois é necessário que haja "falsidade", "dano" e "dolo". Neste caso, a falsidade implica em uma informação objetivamente

[16] *"news articles that are intentionally and verifiably false, and could mislead readers."*

incorreta, que não corresponde à realidade dos fatos de maneira direta e concreta. O dano refere-se ao impacto negativo que a desinformação causa à sociedade, indivíduos ou instituições, enquanto o dolo demonstra a intenção deliberada de enganar ou manipular a opinião pública. Rais enfatiza que esses elementos devem existir para que se possa distinguir entre um erro inocente e uma campanha de desinformação deliberada. Ele ressalta a importância de responsabilizar legalmente aqueles que produzem ou deliberadamente disseminam *fake news* com o objetivo de causar prejuízos ou obter vantagens indevidas.

Convém assinalar que, apesar dos esforços para definir claramente os conceitos de "desinformação" e *"fake news"*, os estudiosos ainda não chegaram a um consenso. Devido à polissemia que ambos os termos compartilham, frequentemente causam confusão. De acordo com o dicionário Merriam-Webster (2024), o vocábulo *fake news* surgiu no final do século XIX, tendo sido mencionado em publicações como *Cincinnati Commercial Tribune* e *The Kearney Daily Hub.* O termo, entretanto, ganhou popularidade em 2016, após eventos políticos como o referendo do *Brexit*[17] no Reino Unido e a eleição de Donald Trump para a presidência dos Estados Unidos (EUA). O termo foi distorcido em seu significado original, que se referia a uma ferramenta usada por políticos, sendo posteriormente associado à imprensa como parte de uma estratégia para desqualificar veículos de comunicação críticos (Allcott; Gentzkow, 2017).

Sobre esse aspecto, diversos autores procuram esclarecer o termo apresentando suas perspectivas. Para Quandt *et al*. (2019), as *fake news* podem ser compreendidas tanto como notícias fabricadas que circulam nas redes sociais quanto como uma expressão usada para desacreditar a mídia tradicional. Gelfert (2018) define o conceito como uma apresentação intencional de informações falsas ou enganosas na forma de notícias. Rini (2017) observa que esses conteúdos imitam as convenções da mídia tradicional, mas são criados com o objetivo de enganar o público. Lazer *et al* (2018) enfatizam que as *fake news* imitam apenas a forma da mídia, não seu processo ou intenção organizacional.

Por causa dessas ambiguidades, alguns Estados, instituições e acadêmicos têm evitado o termo *fake news* por considerarem que há significados muito divergentes que dificultam um entendimento mais conciso do fenômeno relativo à disseminação de informações enganosas. No lugar, eles optaram por utilizar o termo "desinformação" *(disinformation)*, o qual definem como a "criação e troca deliberada de informações falsas e/ou manipuladas com a intenção de enganar o público, seja com o propósito de causar malefícios, seja para fins políticos, pessoais ou econômicos". Esse entendimento segue o estabelecido pela Comissão de Tecnologia Digital,

[17] O *Brexit* foi um movimento político que defendeu a saída do Reino Unido da União Europeia (Evans; Menons, 2017).

Cultura, Mídia e Esporte da Câmara dos Comuns do Reino Unido (*House of Commons*, 2019, p. 10, tradução nossa)[18]. Já para a informação falsa que é compartilhada inadvertidamente, sem a intenção de causar danos, o termo utilizado é "misinformação", ou "informação errônea" *(misinformation).*

Ainda na tentativa de estabelecer alguns parâmetros que contribuam para o entendimento conceitual, Wardle e Derakhshan (2017) introduziram o termo "má informação" *(malinformation)* na tipologia da desordem informacional. Segundo essa nova terminologia, essa "má informação" está relacionada principalmente à intenção do disseminador, sendo entendida como informações corretas, mas compartilhadas maliciosamente de maneira descontextualizada com o intuito de causar danos, geralmente envolvendo dados privados divulgados publicamente sem autorização. Eles destacam que a compreensão sobre as *fake news* frequentemente se confunde nesses três conceitos.

Para diferenciar os conceitos, os autores citam como exemplo de desinformação a divulgação de documentos falsos nas redes sociais relacionados ao então candidato à presidência da França nas eleições de 2017, Emmanuel Macron. Esses documentos forjados levaram a população a crer que Macron tinha uma conta bancária no paraíso fiscal das Bahamas, um país caribenho. A desinformação se espalhou nas redes sociais com o intuito de difamá-lo. Além disso, os difamadores também veicularam informações com rumores sobre um suposto relacionamento de Macron com sua enteada (Wardle; Derakhshan, 2017).

Os autores utilizaram como exemplo de misinformação o ataque ocorrido na *Champs Elysées*, em Paris, no dia 20 de abril do mesmo ano, quando um policial foi morto e outros dois ficaram feridos durante um tiroteio. Nas redes sociais, houve uma disseminação inadvertida de que um segundo policial também havia sido morto. Os autores explicam que esse exemplo mostra como são comuns o compartilhamento de informações erradas em situações de pressão emocional. Geralmente essas informações são compartilhadas sem a intenção de prejudicar, mas, devido à situação e tentativa de ser útil, podem levar à disseminação de informações não verificadas e com erros (Wardle; Derakhshan, 2017).

Um exemplo de "má informação" – quando a informação é verdadeira, mas compartilhada com a intenção de causar prejuízo –, citado pelos autores também está relacionado às eleições presidenciais francesas de 2017. Na ocasião, *hackers* obtiveram documentos internos relacionados a Macron, por meio de e-mails de *phishing*, e vazaram as

---

[18] *"Disinformation refers to the deliberate creation and sharing of false and/or manipulated information that is intended to deceive and mislead audiences, either for the purposes of causing harm, or for political, personal or financial gain".*

informações na tentativa de prejudicar a campanha antes do segundo turno das eleições. Para evitar influências indevidas e garantir a integridade do processo democrático, a imprensa foi proibida de publicar qualquer informação sobre o conteúdo dos documentos. Essa restrição permitiu que os eleitores tomassem decisões sem serem influenciados por potenciais manobras políticas. Donadio (2017) acrescenta que a equipe de Macron adotou como estratégia sobrecarregar os e-mails fraudulentos com informações falsas, tornando difícil para os agentes maliciosos distinguirem o que era verdadeiro do que era falso, impedindo os esforços desses invasores de provocar danos.

2.2.4 Digital astroturfing e criação de falsas verdades

Digital astroturfing deriva de *astroturfing,* que consiste na manipulação da opinião pública por meio da criação de falsos grupos de apoio ou oposição a um determinado assunto. O termo é relacionado à palavra *"astroturf",* um tipo de grama sintética usada em campos esportivos e que simboliza a artificialidade dessa prática. O objetivo desse artifício é convencer o público de que uma opinião é amplamente apoiada por meio de um consenso generalizado sobre determinada questão, quando, na realidade, é apenas uma estratégia de marketing ou propaganda disfarçada. Essa tática abrange comentários em massa em blogs e fóruns, envio de cartas ou e-mails falsos, entre outros recursos (Chan, 2024).

No contexto das redes sociais, o *digital astroturfing* envolve várias abordagens. Isso inclui ocultar a identidade com contas falsas ou pseudônimos. Também envolve usar algoritmos e *bots* para amplificar a mensagem e simular interações humanas com o uso da segmentação da audiência para direcionar mensagens específicas. Muitas das práticas executadas pelos *astroturfers* não se limitam a declarações em *posts* ou comentários. Em algumas situações, essas atividades podem se resumir a simplesmente seguir uma conta em uma determinada rede social ou "curtir" determinados *posts* estrategicamente, compartilhados por um candidato político, por exemplo (Lazarotto, 2023).

2.2.5 Vigilância e manipulação de dados pessoais

A vigilância e manipulação de dados pessoais nas redes sociais têm um profundo impacto em relação à proteção da privacidade individual, levantando também uma série de questões sobre a proteção da informação sensível e seu uso em práticas de atividades maliciosas. Sobre isso, Choi, Park e Jung (2018) sustentam que os usuários experimentam uma fadiga da privacidade no espaço virtual. Para os autores, as pessoas se sentem sobrecarregadas

e estressadas pela necessidade de proteger a privacidade no espaço online, levando-as à exaustão emocional e ao ceticismo. Isso pode ocorrer em virtude da crescente complexidade das configurações de privacidade, da alta ocorrência de violações de dados e da sensação de que os esforços para proteger a privacidade não funcionam, pois há uma falta de controle sobre os dados próprios que estão sendo coletados e como as informações são utilizadas por empresas e plataformas online.

Conhecido como "paradoxo da privacidade", o fenômeno revela que a exposição constante nas redes sociais e a falta de regulamentação podem representar ameaças associadas ao uso indevido de informações pessoais (Choi; Park; Jung, 2018). A manipulação estratégica desses dados sensíveis na esfera da guerra cognitiva emerge como uma questão crítica, transcende as fronteiras dos meios digitais e invade os domínios da política, da sociedade e da democracia contemporânea. Esse processo complexo de exploração da informação pessoal destaca os impactos profundos que a manipulação pode exercer sobre a integridade dos processos democráticos, a confiança nas instituições e a própria natureza da interação humana na era digital (Souza, Gorczevski, 2020).

2.2.6 Operações de Influência e de Retórica

As operações de influência e de retórica (RhetOps, na sigla em inglês) são duas formas de usar a habilidade de comunicação de forma eficaz e persuasiva. No contexto da guerra cognitiva, podem ser empregadas para promover uma ideia ou a imagem de alguém, instituição ou de um Estado; desacreditar ou desmoralizar um adversário; obter apoio de aliados ou de terceiros; ou para disseminar informações falsas que favoreçam interesses próprios.

Segundo Ridolfo e Hart-Davidson (2019),

> os exemplos apontam para as formas como o conhecimento retórico é armado em situações de conflito, com práticas que incluem, mas não se limitam a policiamento de *hashtags*, iniciativas de mineração de dados como a da Cambridge Analytica, ataques físicos e eletrônicos à infraestrutura de rede, uso estatal e militar de redes sociais para a disseminação de propaganda e muito mais (p. 248, tradução nossa)[19].

[19] *"These examples point to the ways rhetorical knowledge is weaponized in conflict situations, with practices that include but are not limited to hashtag policing, data-mining initiatives such as Cambridge Analytica, physical and electronic attacks on network infrastructure, state and military use of social media for the dissemination of propaganda, and more".*

Joseph Nye Jr. (2005) argumenta que o poder de influenciar uma pessoa pode ser baseado na atração e na capacidade de persuadi-la de forma sutil e não óbvia. Sob essa perspectiva, as operações de influência não são baseadas somente na ação direta ou agressiva. Elas podem ser realizadas por meio de narrativas persuasivas, propaganda e manipulação da informação com o objetivo de afetar a percepção e a opinião dos indivíduos. Relacionando isso às redes sociais, esse poder é utilizado para exercer esse tipo de influência por meio da disseminação de narrativas que podem moldar percepções, valores e comportamentos de maneira quase imperceptível.

2.2.7 Recrutamento online e terrorismo

O potencial massivo das redes sociais para o engajamento de causas extremistas, como o terrorismo, é uma realidade preocupante que demanda uma resposta global e coordenada. Ridolfo e Hart-Davidson (2019) alertam para a facilidade com que os grupos terroristas recrutam membros, disseminam propaganda fundamentalista, coordenam ataques e angariam financiamento por meio dessas plataformas. A natureza global e instantânea desses ambientes faz com que o conteúdo terrorista se espalhe rapidamente, chegando a uma grande quantidade de pessoas. Além disso, a potencialidade em criar comunidades online torna mais fácil o processo de radicalização e o fortalecimento de ideologias extremistas.

O uso de ferramentas de identificação de narrativas e padrões semânticos possibilita o reconhecimento dessas ações no ambiente online. A RAND Corporation, uma organização de pesquisa estadunidense, desenvolveu uma ferramenta computacional poderosa que combina métodos de diversas áreas para analisar textos de forma escalável. O RAND-Lex reúne métodos de linguística de *corpus* (grande quantidade de textos), retórica digital e ciência da computação, além de algoritmos de aprendizado de máquina supervisionados e não supervisionados. Esse programa permite a análise de grandes volumes de palavras de forma eficiente e precisa. A suíte foi utilizada para realizar testes de relevância e posicionamento nos discursos do grupo terrorista EI, ou ISIS (*Islamic State of Iraq and Syria)*, fornecendo *insights* sobre as táticas comunicativas e estilísticas empregadas. A ferramenta identificou uma combinação de elementos retóricos e estratégias linguísticas específicas, como o uso intenso de termos religiosos, ênfase em narrativas de batalhas e operações táticas concretas, conhecidas como "*dark interactions", ou* interações obscuras. O RAND-Lex associado a outras táticas possibilita a identificação das "*dark interactions"* (interações obscuras) em redes sociais de forma mais

simples, facilitando a detecção de padrões ocultos de influência (Ridolfo; Hart-Davidson, 2019).

Segundo Câmara (2016) e Moreno (2019), o Estado Islâmico se tornou conhecido por utilizar as plataformas de redes sociais, especialmente o X, como uma ferramenta poderosa para difundir sua propaganda, recrutar novos combatentes e popularizar o grupo entre pessoas que vivem longe do Oriente Médio. Os autores ressaltam que a internet e as redes sociais são importantes para o grupo alcançar seus objetivos, estimulando lobos solitários e simpatizantes a agirem isoladamente em seus países, com o objetivo e ganhar proeminência pública, dirigindo-se tanto para adversários como para simpatizantes. Para Singer e Brooking (2018), o EI reconheceu a importância das redes sociais e dedicou grandes esforços para integrá-las e otimizá-las em apoio às operações no campo de batalha, utilizando-as como uma plataforma de armas autônoma.

No Brasil, a Polícia Federal, em conjunto com informações de inteligência financeira do Coaf (Conselho de Controle de Atividades Financeiras) e análises de inteligência estratégica realiza um trabalho de monitoramento de atividades ilícitas de financiamento de grupos criminosos e extremistas. Ainda que não tenham sido encontrados laços evidentes entre os principais grupos terroristas internacionais e o país, foram identificados alguns casos de radicalização ocasional, principalmente durante as edições dos megaeventos esportivos, como a Copa do Mundo de 2014 e os Jogos Olímpicos de Verão do Rio de Janeiro ocorridos em 2016 (Coaf, 2021). Outro órgão que se dedica a essas questões é a Agência Brasileira de Inteligência (Abin, 2020). A instituição mantém como medida antiterrorista a análise de indicadores de comportamento e de conduta suspeitas, incluindo discursos extremados de ódio e incitação à violência nas redes sociais.

2.2.8 Polarização e divisão social

De acordo com Jaime Settle (2018), a polarização social acontece quando a sociedade se divide entre grupos ideológicos opostos. Embora esse fenômeno realce principalmente as divergências entre partidos, ele vai além da política, afetando também as relações sociais e influenciando a formação das identidades coletivas.

O autor explica que a falta de elementos não verbais nas interações em ambientes virtuais, como gestos e expressões faciais, pode gerar dificuldades na comunicação, aumentando a possibilidade de mal-entendidos. Esse resultado é ainda mais acentuado quando as crenças e ideologias enraizadas estão envolvidas. Além disso, a exposição a opiniões

diferentes tanto pode enriquecer o debate quanto intensificar as divisões preexistentes. Esse processo pode resultar em pensamentos e comportamentos com características extremistas.

A polarização é influenciada pelo viés da confirmação, como observado por Klayman (1995). Esse tipo de viés cognitivo ocorre quando indivíduos tendem a procurar e a dar valor para informações que confirmam suas crenças anteriores e ignoram ou rejeitam as informações contrárias. Essa tendência faz com os sujeitos estejam mais condicionados a dados que reforçam suas perspectivas, resultando, muitas vezes, em julgamentos seletivos e enviesados. Assim, o viés da confirmação passa a influenciar a maneira como as pessoas procuram, interpretam e recordam informações, podendo comprometer a imparcialidade na tomada de decisões, o que contribui para a acentuação da polarização e divisão social.

Conforme destacado por Sorj *et al.* (2018), é possível compreender que os algoritmos de personalização ajudam no viés da confirmação, intensificando a polarização nas redes sociais, desempenhando um papel significativo por meio da formação das chamadas "bolhas de filtro", que isolam o sujeito do contato com o contraditório. Ao personalizar o conteúdo apresentado aos usuários com base em suas interações anteriores, histórico de navegação e preferências individuais, essas bolhas provocam o efeito colateral de restringir a diversidade de perspectivas e informações a que os usuários são expostos.

Ao direcionar o conteúdo de forma seletiva, esses algoritmos tendem a favorecer informações que confirmam as visões e opiniões preexistentes dos usuários, ao mesmo tempo em que limitam a exposição a pontos de vista diferentes. Essa dinâmica produz em uma experiência personalizada, na qual os usuários são frequentemente expostos a conteúdos que reforçam suas crenças e convicções, criando assim uma ilusão de consenso e reforçando suas próprias perspectivas (Sorj *et al.*, 2018).

Para finalizar este capítulo, é fundamental recapitular os conceitos, mecanismos, dinâmicas e efeitos apresentados até o momento. Esses elementos formam um conjunto de ferramentas analíticas essenciais que permitem examinar os casos estudados e auxiliam na construção das etapas seguintes da pesquisa, proporcionando uma visão abrangente da guerra cognitiva.

A elucidação dos vários tipos de guerra, assim como os seus mecanismos, dinâmicas e efeitos, releva a necessidade de acompanhar a complexidade e evolução dos conflitos na era digital. Cada uma dessas guerras possui características próprias e impactos distintos, muitas vezes sobrepostos, refletindo a necessidade de entender e se preparar para os desafios emergentes do ambiente das redes sociais. Esses conceitos ressaltam a necessidade de uma abordagem abrangente e estratégica para que se possa tratar as ameaças e possíveis

oportunidades que surjam nos conflitos centrados na guerra cognitiva. Compreender esses elementos-chave não apenas amplia a visão sobre as guerras contemporâneas, mas também permite entender a necessidade de uma abordagem estratégica que possa mitigar os impactos negativos dessas ameaças.

Outra questão fundamental diz respeito à influência dos algoritmos na curadoria de conteúdo das plataformas digitais. Esse elemento desafiador destaca o potencial desses mecanismos no reforço de ideologias, ao usarem os interesses e comportamentos do usuário para direcionar novas experiências. Além disso, os algoritmos não são totalmente neutros, eles, de certo modo, refletem as referências e ideias preconcebidas de seus programadores. Essa personalização constante do conteúdo é um fator crítico por seu potencial de contribuir com a polarização social ao formar "bolhas" sociais.

Avanços tecnológicos, como algoritmos, inteligência artificial e *big data*, estão remodelando a interação nas redes sociais por meio da coleta e manipulação massiva de dados. Associada a essa realidade, a transição para uma "Era da Hiperinteligência" levanta preocupações sobre o controle humano e os impactos sociais que podem vir a existir com a superação da capacidade humana por sistemas inteligentes. Atualmente, a IA nas redes sociais já facilita a manipulação de opiniões e a disseminação de desinformação, especialmente com o surgimento de *deepfakes* e a utilização de algoritmos neuromórficos, que imitam o processamento de informações do cérebro humano, apresentando desafios significativos para a democracia e a segurança online.

Esse ambiente, carregado por uma sobrecarga de informações, também apresenta outros desafios. Essa "infodemia" de dados – termo cunhado por Rothkopf em 2003 – corresponde analogamente aos impactos de uma epidemia, sendo mais perigosa que o próprio vírus humano por seus efeitos devastadores na cognição humana. Conforme abordado por Toffler em 1970, essa sobrecarga mental leva à desordem cognitiva devido à dificuldade do cérebro de processar grande quantidade de dados. Como consequência, potencializa a polarização por meio da manipulação da opinião pública exposta de forma maciça às *fake news* disseminadas nas redes sociais.

O entendimento do conceito das *fake news*, entretanto, é dificultado pela polissemia existente, prejudicando os debates sobre o tema. Essa mesma falta de clareza acontece com a palavra "desinformação". Quando há mais de um significado para o mesmo termo, há uma grande chance de que os participantes das discussões estejam falando sobre coisas diferentes sem perceber. Essa ambiguidade pode gerar mal-entendidos e desviar a atenção dos pontos principais. Na tentativa de resolver esse problema, especialistas sugerem a diferenciação dos

conceitos para que, com a diferenciação das nuances, os debates e ações contra essas ameaças possam ser conduzidos de forma mais padronizada, evitando esforços desnecessários.

Além das *fake news* e da desinformação, outras estratégias da guerra cognitiva são utilizadas por diversos atores. O *digital astroturfing* é a manipulação da opinião pública através da criação de falsos grupos de apoio ou oposição, levando à ilusão sobre um consenso inexistente. Nas redes sociais, envolve técnicas como contas falsas, uso de algoritmos e *bots* para amplificar mensagens e segmentação da audiência. Essas práticas vão além de declarações falsas, incluindo ações como "seguir" ou "curtir" postagens para influenciar as percepções dos usuários online e gerar adesão a ideia que está sendo disseminada.

Outros artifícios utilizados na guerra cognitiva online são a vigilância e a manipulação de dados pessoais disponíveis nas redes sociais. Apesar dessas manobras apresentarem sérias consequências para a privacidade, os indivíduos acabam não adotando os cuidados necessários para se protegerem dos agentes maliciosos. Essa inércia odes ser explicada pelo "paradoxo da privacidade", proposto por Choi, Park e Jung (2018). Segundo essa teoria, os usuários se sentem desmotivados em relação aos cuidados com suas informações pessoais. Parte disso devido à complexidade das configurações exigidas e também à falta de controle pelas plataformas os dados dos usuários. Essa exposição constante, somada às questões regulatórias, expõe os indivíduos à manipulação estratégica, levando a resultados que ultrapassam o ambiente digital, afetando a política, a sociedade e a democracia.

As estratégias de comunicação persuasiva (RhetOps) são outras iniciativas usadas na guerra cognitiva. Essas operações são empregadas para promover ideias, desacreditar adversários, obter apoio de aliados e espalhar desinformação. Os exemplos incluem o policiamento de *hashtags* para controle e manipulação de informações, iniciativas de mineração de dados, como a da Cambridge Analytica, e o uso de redes sociais por forças armadas e governos para moldar narrativas. Joseph Nye Jr. (2005) observa que esse poder pode ter formas mais sutis de influência, usando atração e persuasão para moldar percepções e opiniões por meio de conteúdo informativo e persuasivo.

As redes sociais fornecem meios para recrutamento, mensagens e propaganda radicalizadas, ataques coordenados e financiamento coletivo para atividades terroristas. Seu alcance global e imediato facilita a disseminação ampla e instantânea de conteúdo extremista. Além disso, o processo de radicalização e fortalecimento de ideologias extremistas é reforçado com a formação de comunidades online, facilitada pela tecnologia virtual.

Além disso, segundo Settle (2018), a polarização política afeta ainda mais as interações sociais e a formação de identidades coletivas. No entanto, essa polarização é acentuada pela

ausência de informações não-verbais nas redes sociais, resultando em câmaras de eco virtuais. Nesse contexto, o viés de confirmação, um fenômeno de busca de informações que confirmam crenças já existentes, contribui para a polarização ao prejudicar a tomada de decisões. Por outro lado, os algoritmos reforçam o efeito da bolha de filtro ao fornecer conteúdo personalizado que confirmam as convicções pessoais dos usuários.

3 ESTRATÉGIAS DIGITAIS: UMA ANÁLISE COMPARATIVA EX-POST FACTO DAS ABORDAGENS DA RÚSSIA, CHINA E CAMBRIGE ANALYTICA

O uso das redes sociais como ferramenta da guerra cognitiva, empregada por uma variedade de agentes, como Estados e atores privados, emergiu como uma estratégia atual para influenciar opiniões e manipular a percepção pública em escala global. Ao contrário dos meios de comunicação tradicionais, essas plataformas permitem a disseminação de informações sem a moderação de terceiros, verificação dos fatos ou análise de um mediador, facilitando ainda mais a manipulação da narrativa por qualquer pessoa. De acordo com Allcott e Gentzkow (2017), um usuário comum dessas redes pode atingir uma audiência significativa, comparável aos grandes veículos de comunicação.

A disseminação generalizada da desinformação tem se tornado um desafio crescente para governos e sociedades democráticas. Quando efetuada por agentes de Estado e corporações privadas, a questão se torna ainda mais desafiadora, principalmente porque esses atores possuem as competências e recursos necessários para manipular grandes narrativas e, desta forma, impactar a opinião pública, influenciar comportamentos e minar a confiança nas instituições (Althuis; Haiden, 2018).

Para compreender essas estratégias, este capítulo apresenta uma investigação *ex-post facto* combinada com uma análise comparativa das estratégias adotadas pela Rússia, China e Cambridge Analytica nas redes sociais, no contexto da guerra cognitiva. O método *ex-post facto* é uma abordagem de pesquisa utilizada nas ciências sociais para investigar relações de causa e efeito com base em eventos ou condições que já ocorreram. Ao contrário de um experimento tradicional, onde as variáveis são controladas pelo pesquisador, neste método, as variáveis independentes não são manipuladas, pois a investigação é realizada após o fato ter acontecido. Em vez de manipular as variáveis, o pesquisador observa e analisa as relações entre aquelas existentes (McMillan; Schumacher, 2006).

3.1 ETAPAS DO MÉTODO EX-POST-FACTO

No estudo *ex-post facto*, os dados retrospectivos são analisados para identificar e comparar dois ou mais grupos que diferem em uma variável-chave. A finalidade é verificar as diferenças em suas abordagens e identificar padrões e tendências que possam ajudar a compreender as estratégias adotadas (McMillan; Schumacher, 2006). Nesta pesquisa, foi utilizada uma abordagem descritiva e analítica com foco na variável-chave “estratégia de guerra

cognitiva". A ênfase foi na identificação de padrões, sem a necessidade de estabelecer uma causalidade direta entre as ações realizadas e seus resultados.

As etapas observadas, segundo o método, incluíram a seleção dos grupos, delimitação do problema, contextualização do fenômeno, definição das variáveis independentes, coleta de dados e análise e interpretação dos dados, com base nas recomendações dos autores. Durante a análise, os casos estudados foram comparados para identificar as semelhanças e diferenças nas estratégias adotadas pelos grupos. Essa comparação permitiu não apenas identificar os padrões existentes, mas também destacar as características específicas de cada ator, proporcionando uma compreensão mais profunda dos meios aplicados em diferentes contextos de guerra cognitiva. Procurou-se, com estra triangulação, contrastar casos em que o mesmo fenômeno ocorreu, mas com diferentes estratégias e táticas, a fim de compreender a diversidade de possibilidades da manipulação cognitiva nas redes sociais.

Émile Durkheim (1995), um dos primeiros a utilizar o método comparativo nas ciências sociais, postulava que essa abordagem é adequada quando o número de casos é pequeno e os dados não podem ser controlados experimentalmente. Ele defendia a comparação de semelhanças e diferenças entre fenômenos sociais para se chegar a generalizações. Para Lijphart (1971), o método comparativo é especialmente útil quando há a impossibilidade de utilização do método estatístico, devendo ser aplicado para estudo de fenômenos sociais e políticos complexos, singulares ou com forte dependência do contexto histórico.

3.1.1 Seleção dos grupos

A seleção dos grupos para esta análise *ex-post facto* envolveu a identificação de agentes estatais e não-estatais que empregaram táticas de guerra cognitiva nas redes sociais, com foco particular na Rússia, China e Cambridge Analytica. Esses grupos foram escolhidos com base em suas abordagens distintas em relação à manipulação da opinião pública, considerando as variáveis independentes que influenciaram suas ações.

Para garantir a comparação e evitar a parcialidade, consideraram-se os fatores políticos envolvidos, juntamente com os tipos de plataformas utilizadas e as estratégias de propagação de desinformação empregadas por essas entidades. Essa seleção criteriosa foi feita visando permitir uma comparação mais precisa das técnicas adotadas. Adicionalmente, a escolha buscou oferecer uma compreensão amplificada das complexidades presentes na guerra cognitiva e seus impactos na segurança e estabilidade das democracias atuais.

3.1.2 Delimitação do problema

A utilização de táticas de guerra cognitiva nas redes sociais é um tema que a literatura tem considerado como um fenômeno e que tem sido associado à atuação da Rússia e da China. De acordo com Molter e DiResta (2020), essa prática está se tornando cada vez mais preocupante no cenário internacional. Essa questão se torna ainda mais desafiadora na medida em que as agências de inteligência desses países passaram a ter um papel central na propagação de *fake news* e da desinformação, ao explorar as fragilidades das plataformas digitais como um novo campo de batalha. As pesquisas recentes desses autores, juntamente com as de Barnes e Sanger (2020), têm destacado essa tendência de emprego de estratégias de manipulação por diferentes atores estatais. Da mesma forma, Cadwalladr e Graham-Harrison (2018) revelaram a atuação de atores privados, com a Cambridge Analytica, nessas estratégias, levantando questionamentos acerca da capacidade das democracias contemporâneas de prevenir e enfrentar a guerra cognitiva nas plataformas de redes sociais.

Considerando as evidências apresentadas, esta análise, baseada em métodos *ex-post facto* e análise comparativa, busca identificar quais as estratégias e impactos da guerra cognitiva empreendida pela Rússia, China e Cambridge Analytica nas redes sociais, e como essas ações interferem na estabilidade política das democracias contemporâneas. Além disso, o método comparativo procura compreender como essas estratégias se assemelham e se diferenciam. contribuindo para um entendimento mais robusto das suas dinâmicas e impactos.

O estudo parte da hipótese de que as práticas de guerra cognitiva desses atores nas redes sociais podem ser utilizadas em outros contextos sociais, com implicações profundas para a estabilidade política e a segurança das democracias contemporâneas. Além disso, indica que as diferenças nas abordagens dessas entidades oferecem lições valiosas que podem ser aplicadas para fortalecer as democracias contra a manipulação e a desinformação.

3.1.3 Contextualização do fenômeno

Nesse novo cenário, países como a Rússia e a China têm adotado sistematicamente as redes sociais para disseminar desinformação, distorcer fatos e promover narrativas que atendam aos seus interesses calculados. Por meio de campanhas coordenadas e financiadas, esses agentes buscam fragilizar a confiança nas instituições e governos estrangeiros, semear a discórdia e moldar a opinião pública em seu favor. A utilização estratégica das redes sociais nesse contexto tem impactos significativos na política externa e nas relações internacionais, além do âmbito

doméstico, representando um desafio crescente para a segurança e estabilidade global (Barnes; Sanger, 2020).

Utilizando estratégias de guerra cognitiva, a Cambridge Analytica se destacou de forma polêmica nas discussões sobre o *Brexit* e nas eleições presidenciais dos EUA em 2016. A empresa usou técnicas de microsegmentação e análise de dados para manipular a opção política dos eleitores. No caso do *Brexit*, ela ajudou a criar e disseminar mensagens que ajudaram na vitória do grupo *Leave.EU*, que estava a favor da saída do Reino Unido da União Europeia. De maneira semelhante, nas eleições americanas, a empresa recorreu a dados pessoais de usuários de redes sociais para direcionar suas campanhas e anúncios políticos, o que acabou intensificando divisões sociais e influenciando o resultado da eleição (Cadwalladr, Graham-Harrison, 2018).

Diversos sistemas e métodos têm sido utilizados nas redes sociais para potencializar a guerra cognitiva. Uma pesquisa conduzida por Li, Vasarhelyi e Vedres (2024) identificou um aumento significativo na atividade de "bots sociais" nessas plataformas. As autoras afirmam que esse ecossistema híbrido de interação dos usuários com esses agentes algorítmicos tem gerado consequências relevantes no discurso online, ajudando a gerar um sentimento subsequente mais negativo nos usuários, que é mais frequente naqueles que estão expostos a interações por a *bots*.

De acordo com a análise, realizada em *posts* do X, foram identificados diferentes tipos de *bots* em ação, como os *bots* de *astroturfing* político, utilizados para influenciar o sentimento humano em relação aos protestos da *Extinction Rebellion* (XR), um movimento global de ativismo climático que usa ação direta não-violenta. Esses *bots* dotados de inteligência artificial foram utilizados para amplificar mensagens favoráveis ou desfavoráveis ao movimento, com o objetivo de manipular a percepção pública e moldar o debate em torno das questões climáticas. "Tais *bots* são frequentemente projetados para passar como contas humanas e, ocasionalmente, imitam explicitamente figuras políticas conhecidas e contas do governo para ganhar a atenção e a confiança de usuários humanos" (Li; Vasarhelyi; Vedres, 2024. s.p., tradução nossa)[20].

Um outro estudo expôs a estratégia de manipulação em massa utilizada por governos, empresas de relações públicas e partidos políticos nas redes sociais. Segundo o Inventário Global de Manipulação Organizada da Mídia Social 2020, do Oxford Internet Institute (OII), esses agentes estão produzindo desinformação nas redes sociais de maneira industrializada e

---

20 "Such bots are frequently designed to pass as human accounts, and occasionally explicitly mimic known political figures and government accounts to gain the attention and trust of human users".

profissional. A pesquisa analisou 81 países e identificou ocorrência de campanhas coordenadas de manipulação em todos eles, inclusive no Brasil (Bradshaw; Bailey; Howard; 2021).

O levantamento encontrou ações de manipulação da informação realizadas por grupos estruturados, indicando uma estratégia coordenada para influenciar a percepção pública e direcionar o discurso. Em uma escala de três níveis (alta, média e baixa) utilizada para avaliar o emprego dessas "tropas cibernéticas", o Brasil foi classificado como de média capacidade, ao lado de outros países como Armênia, Austrália, Bolívia, Cuba, Hungria, Polônia, México, Síria e Turquia. As equipes de média capacidade são caracterizadas por terem uma forma e estratégia mais consistentes, com membros dedicados em tempo integral, durante todo o ano, para controlar o espaço da informação. Essas equipes frequentemente realizam as ações de forma coordenada com vários tipos de atores, e utilizam uma ampla variedade de ferramentas e estratégias para manipulação nas redes sociais. Algumas equipes de média capacidade praticam operações de influência no exterior, o que significa que estão envolvidas em atividades de manipulação nas plataformas digitais em outros países (Bradshaw; Bailey; Howard; 2021).

As estratégias mais utilizadas foram mensagens pró-governo, ataques à oposição e polarização. Esses grupos organizados, compostos por agências governamentais, partidos políticos, empresas privadas ou influenciadores, foram responsáveis por disseminar propaganda, ataques online e "desinformação de aluguel" para influenciar debates políticos, eleições e a percepção. Os dados da pesquisa indicam que a disseminação de desinformação em larga escala aumentou em 15% nos países examinados, em comparação a 2019, quando foram identificados casos em 70 países diferentes. De acordo com o relatório, a prática se tornou uma estratégia comum, com mais de 93% dos países (76) reconhecendo que a desinformação é utilizada como parte da comunicação política (Bradshaw; Bailey; Howard; 2021).

Como alertam os autores, esse aumento no nível de manipulação das redes sociais é impulsionado por significativos investimentos de governos e partidos políticos. Eles financiam empresas privadas para utilizarem suas forças cibernéticas com o propósito de suprimir determinadas narrativas nas plataformas online. Em 2020, esses investimentos totalizaram cerca de US$ 10 milhões globalmente. Para atender a essa estratégia, essas empresas recrutam influenciadores, incluindo voluntários, grupos de jovens e organizações da sociedade civil, para propagarem informações tendenciosas e falsas, ou fazer ressoar determinadas mensagens intencionalmente em câmaras de eco (*eco chambers)* (Bradshaw; Bailey; Howard; 2021).

O estudo revelou que, nas campanhas de disseminação de desinformação, foram utilizadas técnicas de propaganda, ferramentas computacionais e contas falsas com *bots*, além de usuários humanos e contas hackeadas. O relatório concluiu que 76 países faziam uso da

desinformação e da manipulação em suas campanhas, enquanto 30 países usaram dados para enviar anúncios políticos a usuários específicos, e 59 recorreram a *trolls* (usuários perturbadores e provocativos) financiados pelo Estado para atacar opositores políticos ou ativistas (Bradshaw; Bailey; Howard, 2021). A utilização conjunta dessas técnicas revelou a evolução constante na sofisticação das operações de influência digital, conforme estruturado na Tabela 1.

Tabela 1 – Métodos de manipulação em redes sociais (2020)

MÉTODOS DE MANIPULAÇÃO NAS REDES SOCIAIS	Nº DE PAÍSES
Contas humanas	79
Desinformação e manipulação da mídia	76
Trolls patrocinados pelo Estado	59
Contas de *bots*	57
Movimentação de dados para anúncios políticos	30
Contas *hackeadas* ou roubadas	14

Fonte: Elaborado pela autora, com base em Bradshaw, Bailey e Howard (2021).

Neste domínio digital, a China e a Rússia tornam-se intervenientes importantes devido à sua expertise em tecnologia e estratégias cibernéticas concebidas para moldar o cenário geopolítico global (Geers, 2015). A aceleração da mudança da influência econômica dos Estados Unidos e da União Europeia para os países asiáticos, particularmente com a China e a Rússia intensificando seus esforços na revisão desse *status quo*, evidencia a importância crescente destas nações na redefinição das estruturas de poder globais. Viola e Lima (2013) explicam que essas iniciativas fazem parte de um plano mais amplo para desafiar o domínio do mundo ocidental e criar regras e dinâmicas de poder que se alinhem com os seus objetivos e prioridades estratégicas.

A escolha desses países como focos desse estudo está fundamentada na ampla evidência das suas atividades intensas e relevantes no âmbito da guerra cognitiva nas redes sociais. Ambos os Estados têm sido acusados de interferir em assuntos políticos e eleitorais em várias regiões do mundo. Graças à sua avançada expertise em tecnologia e estratégias cibernética, eles possuem a capacidade de exercer uma influência significativa no cenário geopolítico global. Numerosos estudos e relatórios têm destacado as capacidades de executar campanhas altamente sofisticadas de manipulação da informação e desinformação nas redes sociais (Barnes; Sanger, 2020; Molter; DiResta, 2020; Anwar, 202; Kelton *et al*., 2019).

A Rússia, por exemplo, é conhecida por utilizar técnicas de manipulação da informação através de sites secretos, redes sociais, *bots* on-line e *trolls* para disseminar narrativas pró-Kremlin e exercer influência em outras nações (Conley *et al*., 2020). Da mesma maneira, a China faz uso das redes sociais para espalhar mensagens explícitas e realizar campanhas coordenadas de desinformação, buscando influenciar narrativas e opiniões. O objetivo é estigmatizar qualquer crítica à sua política e favorecer uma visão positiva de suas ações, aproveitando-se da polarização e desconfiança causadas pela desinformação para influenciar a percepção sobre questões políticas e internacionais (Zhang, 2021).

Nesse contexto, a pesquisa tem como objetivo analisar como essas estratégias são aplicadas e entender as consequências dessas ações em um mundo cada vez mais influenciado pela comunicação digital e pela manipulação de informações. Em um novo ambiente de domínio multipolar, a aliança conjuntural entre a China e a Rússia têm ampliado a influência global desses Estados e recebido atenção no debate geopolítico em geral (Cowman; Hernandez; Sigh, 2023; Mahbubani, 2013; Diesen, 2017).

Além da profundidade e extensão das estratégias de guerra cognitiva, essas ações têm um impacto relevante no cenário internacional. Esses países são exemplos reconhecidos de como a manipulação de informações pode ser usada como uma estratégica geopolítica. tornando-os exemplos significativos que merecem uma análise mais minuciosa no contexto da guerra cognitiva. A manipulação cognitiva está presente em todas as esferas da interação internacional, indo além das campanhas eleitorais ou conflitos militares. Ela perpassa as negociações diplomáticas atingindo até disputas comerciais. Compreender essas dinâmicas é de fundamental importância para desenvolver contramedidas que protejam a integridade das informações nas sociedades em uma realidade cada vez mais interconectado.

3.1.4 Definição das variáveis independentes

De acordo com McMillan e Schumacher (2006), a seleção das variáveis é essencial para determinar o objeto de investigação e responder aos questionamentos do estudo. Com o objetivo de analisar as estratégias empregadas pela Rússia, China e Cambridge Analytica na guerra cognitiva nas redes sociais, foram selecionadas variáveis que levam em conta a compreensão das dinâmicas de manipulação da informação e os impactos dessas práticas nas democracias atuais para todos esses atores envolvidos. Segundo Creswell (2014), as variáveis independentes em pesquisa qualitativa são elementos contextuais, individuais e processuais que influenciam os fenômenos estudados. No contexto desta pesquisa, foram selecionados o contexto político e

social, a dinâmica das redes sociais, as estratégias de manipulação, o uso de informações pessoais, e as ações de agências de inteligência.

3.1.4.1 Contexto político e social

Uma variável independente significativa é o contexto político e social em que as campanhas de guerra cognitiva ocorrem. Divisões políticas, desconfiança nas instituições e instabilidade democrática são elementos que favorecem a manipulação e podem intensificar a disseminação da desinformação com o propósito de desestabilizar o ambiente democrático. O estudo examina o contexto histórico e social de cada um dos países, para identificar como essas condições podem influenciar a receptividade do público a narrativas manipuladoras.

3.1.4.2 Dinâmica das redes sociais

As redes sociais são ambientes profícuos para a disseminação da desinformação e *fake news*. Este estudo analisa como os elementos e dinâmicas característicos desses ambientes favorecem as táticas de guerra cognitiva e a propagação viral de narrativas enganosas, pelos atores estudados, com o propósito de influenciar a opinião pública. Além disso, examina os efeitos dessas práticas na sociedade e na confiança nas instituições democráticas.

3.1.4.3 Estratégias de manipulação

Esta variável diz respeito a estratégias específicas utilizadas pelos atores para influenciar as opiniões e comportamentos. Isso inclui a disseminação de desinformação, promoção de propaganda segmentada e direcionamento de mensagens personalizadas *(microtargeting).* O estudo procura identificar como essas táticas são ajustadas a diferentes ambientes culturais e políticos.

3.1.4.4 Uso de informações pessoais

A coleta e o uso de dados pessoais foram estratégicos para a efetividade da estratégia da Cambridge Analytica, permitindo segmentar o público-alvo de maneira precisa. A análise dessa variável explora como os dados demográficos, psicológicos e comportamentais podem ser usados para dividir os eleitores em grupos e criar campanhas adaptadas às necessidades

específicas de cada um deles. A utilização desses dados coletados de plataformas de redes sociais populares, como o Facebook, foi alvo principal de investigação, particularmente no que diz respeito às implicações éticas e jurídicas relacionadas a essa prática.

3.1.4.5 Ações de agências de inteligência

O papel das agências de inteligência na propagação de desinformação, especialmente a da China e da Rússia, é uma das variáveis investigadas. A pesquisa procura analisar como esses órgãos estatais empregam campanhas nas redes sociais para interferir em eleições e orientar a narrativa em favor de seus próprios interesses. Foram avaliadas operações específicas para analisar seus efeitos na soberania e segurança nacionais. Com o estudo mais aprofundado dessas variáveis independentes, é possível entender melhor as relações das estratégias de guerra cognitiva e seus resultados sobre as democracias contemporâneas.

3.1.5 Coleta de dados

O estudo usou a pesquisa bibliográfica sobre as variáveis que influenciam a guerra cognitiva, como método para coletar informações. A revisão analisou artigos acadêmicos, livros e relatórios sobre as atividades online da Rússia, China e Cambridge Analytica. Foram selecionadas fontes que abordavam táticas de manipulação nas redes sociais e seus impactos nas democracias dos contextos analisados. Apenas trabalhos que apresentavam métodos rigorosos e resultados bem fundamentados foram considerados.

3.2 ESTUDO EX-POST FACTO SOBRE AS ESTRATÉGIAS DIGITAIS RUSSAS

4.2.1 Contextualização histórica da guerra cognitiva na Rússia

A guerra cognitiva na Rússia tem raízes em contextos históricos profundos e está intimamente ligada à estratégia militar e de influência do país. Tradicionalmente, o Estado tem empregado a “Maskirovka”, doutrina militar que se baseia em métodos de engano e ocultação, como parte de suas táticas de guerra para camuflar as intenções e ações (Dąbrowska, 2022). Além disso, o país é conhecido por suas *“Active Measures”* (Medidas Ativas), que envolvem operações de desinformação, propaganda e manipulação da opinião pública com o objetivo de atingir metas políticas e estratégicas. Essas práticas têm sido fundamentais na forma com o país

lida com conflitos no cenário internacional. O propósito em utilizar essas táticas é criar uma atmosfera de incerteza e confusão, tornando difícil para os usuários estabelecerem a diferença entre o que é verdadeiro do que é falso, moldando, desta forma, suas percepções e comportamentos de acordo com os objetivos pretendidos (Kux, 1984).

Soldatov e Borogan (2015) discutem que, ao longo da Guerra Fria (1947-1991), a União Soviética fez uso intenso da propaganda como um recurso para moldar a opinião pública, tanto interna quanto externamente. A mídia estatal, sob controle do governo soviético, gerenciava a narrativa, veiculando informações que favoreciam os interesses do regime comunista e desmerecendo as potências ocidentais. A manipulação da informação constituiu uma tática fundamental para assegurar o domínio sobre a população e para rivalizar com os Estados Unidos e seus aliados.

Os autores apontam que, após o colapso da União Soviética em 1991, a Rússia enfrentou uma série de desafios, tanto no âmbito econômico quanto no político. Nesse período de transição, emergiram grupos de oligarcas que passaram a controlar os principais veículos de comunicação, influenciando a narrativa pública para atender a seus próprios interesses financeiros e políticos. A liberdade de imprensa sofreu restrições frequentes, e o governo russo exercia uma influência indireta sobre os meios de comunicação através de diversos mecanismos legais e econômicos (Soldatov; Borogan, 2015).

Em 2014, durante a anexação da Crimeia, a Rússia passou a intensificar o uso das redes sociais como arma de guerra. Esse evento marcou um ponto de inflexão no emprego estratégico das plataformas digitais por um Estado em um conflito geopolítico. Desde então, houve uma maior sofisticação e disseminação de campanhas informacionais nas redes sociais como arma de guerra estatal (Jaitner; Mattsson, 2015).

Segundo Holloway (2017), o governo russo investiu nesse conflito mais de US$ 19 milhões para financiar centenas de pessoas em uma operação de manipulação de informações nas redes sociais. Esse "exército virtual" tinha a tarefa de comentar constantemente em artigos noticiosos, escrever blogs e se engajar ativamente em redes sociais, disseminando uma narrativa favorável à anexação da Crimeia pela Rússia. O *digital astroturfing* foi usado com o objetivo de criar a impressão de que havia um apoio massivo da população local à anexação, mesmo que isso não correspondesse à realidade.

Esse evento seminal na Crimeia impulsionou ainda mais os interesses e estratégias da Rússia no ambiente informacional. No início dos anos 2000, o presidente Vladimir Putin consolidou ainda mais o controle sobre a mídia, limitando a independência dos veículos de comunicação e fortalecendo o papel da imprensa estatal. Paralelamente, a Rússia começou a

expandir suas operações de guerra cibernética e de propaganda. A utilização de *trolls, bots* e mídia financiada pelo Estado se tornou uma estratégia comum para influenciar debates políticos em todo o mundo e desestabilizar governos ocidentais (Soldatov; Borogan, 2015).

Em seu discurso proferido na Academia de Ciências Militares da Rússia, em março de 2018, o Chefe do Estado-Maior Geral das Forças Armadas da Federação Russa e Primeiro Vice-Ministro de Defesa, Valery Gerasimov, destacou o direcionamento para "alvos econômicos e sistemas de controle estatal", além da "esfera" e do "espaço informacionais" como prioridades das guerras futuras:

> Cada conflito militar tem, indiscutivelmente, suas próprias características distintivas. [...] Os alvos econômicos e o sistema de controle estatal do inimigo serão visados como objetivos prioritários de destruição. Além das esferas tradicionais da luta armada, a esfera e o espaço informacionais serão envolvidos dinamicamente (Orenstein, 2019).

Gerasimov já havia abordado em 2013 que as ações militares e não militares – subdivididas em políticas, sociais, econômicas, informacionais, tecnológicas, diplomáticas e de guerra – deveriam trabalhar de forma coordenada com o mesmo propósito (Orenstein, 2019).

4.2.2 Manipulação e desinformação russa nas redes sociais

A atuação da propaganda russa nas plataformas digitais frequentemente recorre a narrativas que envolvem teorias da conspiração e a disseminação de informações enganosas. O intuito dessas ações é minar a confiança nas instituições democráticas e incitar a desordem social. Tais estratégias podem envolver a propagação de teorias da conspiração relacionadas a eventos globais, como ataques terroristas ou pandemias, com a finalidade de criar discórdia e confusão entre os diferentes públicos-alvo. Além disso, conforme discutido por Soldatov e Borogan (2015), a Rússia tende a explorar as divisões sociais e políticas já existentes em outras nações. O objetivo é intensificar conflitos e polarizações. Essa abordagem inclui o suporte a grupos extremistas, a promoção de agendas separatistas e o enfraquecimento da coesão social, por meio da difusão de mensagens que fomentam a divisão social e que são, em sua essência, inflamadas.

Os autores afirmam, ainda, que a Rússia emprega uma variedade de *bots* e *trolls* nas redes sociais para disseminar mensagens tendenciosas, amplificar conteúdo favorável ao Kremlin e desacreditar fontes de informação críticas ao governo russo. Essas contas

automatizadas e perfis falsos são usados para criar a impressão de apoio popular a certas políticas ou figuras da sociedade, e para semear divisões em sociedades estrangeiras.

Essas campanhas de desinformação, que são comandadas pela agência de inteligência militar *Glavnoye Razvedyvatel'noye Upravleniye* (GRU), têm como propósito, segundo revelam os autores, fragilizar a confiança dos cidadãos nas instituições e processos democráticos. Ao criar narrativas que questionam a integridade dos sistemas eleitorais, a eficácia dos órgãos governamentais e a credibilidade da mídia convencional, essas operações buscam suscitar dúvidas e ceticismo entre a população. A estratégia é abalar a confiança pública nas estruturas e mecanismos fundamentais da democracia, minando a crença da sociedade no processo político e nas fontes de informação confiáveis para desestabilizar a ordem democrática e enfraquecer a unidade social (Soldatov; Borogan, 2015).

A interferência em processos eleitorais e na democracia de outros países é um elemento importante da estratégia de propaganda russa nas plataformas digitais, como destacam Soldatov e Borogan (2015). As táticas utilizadas podem incluir a divulgação de informações prejudiciais sobre candidatos, a disseminação de desinformação relacionada aos procedimentos eleitorais e a tentativa de influenciar os resultados das eleições por meio da manipulação da percepção pública. Além disso, a propaganda russa se destaca frequentemente pela criação de identidades falsas e fontes de informação enganosas, tornando difícil para os usuários distinguirem entre conteúdos autênticos e manipulados. Métodos como a criação de sites de notícias fraudulentos, o uso de perfis fictícios em redes sociais e a disseminação de conteúdos enganosos por meio de contas que parecem legítimas são algumas das estratégias empregadas nessa batalha cognitiva.

No início de 2017, a Comunidade de Inteligência dos Estados Unidos (IC, na sigla em inglês) concluiu que o Kremlin usou a GRU em uma campanha de influência durante as eleições presidenciais estadunidenses de 2016. Os três principais objetivos dessa campanha eram minar a confiança pública na democracia dos Estados Unidos, difamar a secretária de Estado Hilary Clinton e desestabilizar a sua candidatura, favorecendo o candidato Donald Trump. A IC chegou à conclusão de que, durante o período eleitoral, houve uma clara preferência russa em apoiar Trump, com o intuito de aumentar suas chances de vitória. Essas ações desempenharam um papel significativo na influência exercida sobre o processo eleitoral (Intelligence Community Assessment, 2017; Sanger, 2018).

No contexto do conflito armado na Ucrânia, a Rússia utilizou diversas estratégias de manipulação da informação com a finalidade de alterar a percepção pública e promover seus propósitos políticos. Um relatório do Atlantic Council (2023) revela que os russos disseminaram rumores sobre corrupção política e vendas de armas ocidentais no mercado negro

internacional pelo governo ucraniano. Isso foi feito por meio de postagens enganosas que circularam em plataformas de redes sociais. Vídeos e áudios foram editados e reinterpretados para induzir a desconfiança e gerar pânico, aprofundando a confusão e a desinformação entre os usuários dessas plataformas.

As atividades das agências de inteligência russas foram determinantes no planejamento da invasão, conduzindo operações de desinformação. Eles foram responsáveis por influenciar a opinião pública e fragilizar a confiança nas instituições para desestabilizar a Ucrânia. A coordenação entre o Serviço de Inteligência Estrangeira (SVR) e o Serviço Federal de Segurança (FSB) russos utilizada pelo Kremlin para a execução da estratégia militar. As agências agiram conjuntamente como uma frente coesa, compartilhando seus recursos e informações para amplificar o efeito das ações do governo russo, usando várias plataformas online na disseminação da desinformação (Giles *et al*, 2023).

Uma estratégia utilizada pela Rússia, segundo Monnerat (2024), foi a propagação da notícia falsa de que o presidente ucraniano, Volodymyr Zelenski, estaria comercializando armas com o Oriente Médio para abastecer o grupo extremista Hamas. A venda teria triplicado nos últimos anos, demonstrando um ato contínuo nessa atividade. Essas narrativas enganosas visavam enfraquecer a estabilidade política do país e semear a desconfiança na população em relação às autoridades. Além de criar uma percepção negativa da Ucrânia no cenário internacional, buscou atingir sua credibilidade e legitimidade como ator no conflito.

3.3 ESTUDO EX-POST FACTO SOBRE AS ESTRATÉGIAS DIGITAIS CHINESAS

3.3.1 Contextualização histórica da guerra cognitiva na China

Identificar sinais históricos da guerra cognitiva na China representa um desafio complexo e difícil de ser alcançado, principalmente devido à natureza sutil das estratégias utilizadas nas diversas guerras internas entre as dinastias, muitas vezes sem deixar documentação explícita. Como uma nação milenar, a China passou por uma série de conflitos domésticos que contribuíram significativamente para a evolução e o refinamento das estratégias militares empregadas ao longo dos séculos (Zhongqiu, 2023).

Um importante líder militar, que se destaca na evolução estratégica chinesa, e cujas diretrizes contribuíram significativamente para a formação do pensamento militar, é o renomado general e estrategista Sun Tzu. Nascido por volta de 545 a.C., Sun Tzu se destacou por sua capacidade de desenvolver estratégias militares que transcendem as fronteiras do tempo

e continuam a influenciar líderes e estrategistas em diversas áreas até os dias de hoje (Sun Tzu Art of War, 2023).

Seu conhecimento sobre a arte da manipulação cognitiva, revela quão profundas e complexas são as técnicas empregadas desde tempos antigos. Em sua milenar obra "A Arte da Guerra", Tzu (2017) destaca a importância do uso estratégico da informação como uma ferramenta fundamental para alcançar a vitória no campo de batalha. Ele afirmava que a "lei da guerra se baseia no engano" (p. 36), evidenciando que o sucesso nas campanhas militares depende de artifícios que permitem superar as forças inimigas. Isso envolve a capacidade de iludir o oponente deixando-o vulnerável por meio da astúcia e da surpresa. A sabedoria de Tzu ainda ressoa hoje, lembrando de que a manipulação da informação pode ser uma arma poderosa em diversos contextos.

A ascensão chinesa contemporânea encontra em Mao Tsé-Tung outra figura emblemática. O líder político, que fundou o Partido Comunista Chinês (PCC) e liderou a transformação da China para uma república popular, reflete em suas doutrinas a influência de Sun Tzu, enfatizando a importância do controle da narrativa e da propaganda para consolidar o poder e influência do PCC. Ao declarar que, "para alcançar a vitória, devemos, na medida do possível, tornar o inimigo cego e surdo, selando seus olhos e ouvidos, e levar seus comandantes à distração, criando confusão em suas mentes" (Yoshihara, 2011, p. iii, tradução nossa)[21], Tsé-Tung deu ênfase à importância do uso da informação como ferramenta estratégica. O estadista influenciou a forma como as teorias militares modernas consideram a relevância da informação na condução de operações militares e na busca pela vantagem sobre o inimigo.

De acordo com Herrera (2022), as atuais políticas do presidente chinês Xi Jinping são influenciadas pela herança de Mao Tsé-Tung. A Revolução Cultural e outras políticas de Mao moldaram a China contemporânea e ainda afetam seu governo. No governo Xi, a China utiliza estratégias de guerra cognitiva para fortalecer seu controle interno, melhorar sua reputação internacional e proteger seus objetivos estratégicos.

3.3.2 Manipulação e desinformação chinesa nas redes sociais

A China desenvolveu o Domínio Cognitivo de Operações (CDO, na sigla em inglês), um conceito que visa utilizar a informação para influenciar as funções cognitivas de um adversário, abrangendo desde a opinião pública em tempos de paz até a tomada de decisões em

[21] *"To achieve victory we must as far as possible make the enemy blind and deaf by sealing his eyes and ears, and drive his commanders to distraction by creating confusion in their minds."*

tempos de guerra. O CDO representa uma evolução da guerra psicológica tradicional, agora incorporando tecnologias de informação avançadas para influenciar a percepção e as decisões do inimigo através da disseminação ideológica, minando o moral e a coesão das tropas adversárias, além de influenciar e moldar suas capacidades operacionais. Esta estratégia se divide em duas categorias principais: cognição, que envolve o uso de tecnologias para impactar a capacidade de pensamento e funcionamento de um indivíduo; e cognição subliminar, que inclui tecnologias destinadas a afetar as emoções, o conhecimento, a força de vontade e as crenças fundamentais de uma pessoa (Beauchamp-Mustafaga, 2019).

A modernização militar chinesa tem se concentrado desde os anos 1990 em buscar uma estratégia de informatização (Silva, 2016). Através dessa iniciativa, o Exército de Libertação Popular (人民解放军 Rénmín Jiěfàngjūn, ou ELP) vem se dedicando a aprimorar suas capacidades de operações de informação, incluindo a guerra cibernética, guerra eletrônica e guerra psicológica. Documentos do ELP sugerem um interesse em desacreditar a liderança e desestabilizar o moral do inimigo, influenciando a percepção, a opinião pública e a psicologia dos adversários. Os estrategistas chineses ressaltam a importância de disseminar todos os tipos de rumores e informações para conquistar as mentes e manipular as percepções e crenças dos indivíduos e grupos-alvo. Essa abordagem estratégica revela a compreensão da China sobre o poder da desinformação e da manipulação da narrativa como instrumentos de guerra não convencional. Ela se estende de forma contínua durante as fases do conflito, abrangendo missões estratégicas, operacionais e táticas, incluindo detectar alvos, executar ataques precisos e ocultar intenções (Zhang, 2021; Red Diamond, 2021).

Um artigo publicado pelo Ministério da Defesa Nacional da China discute o papel das redes sociais como um campo de batalha adicional em conflitos modernos, ao lado do teatro de operações convencional. De acordo com o exposto no documento, "O 'controle invisível' das mídias sociais no planejamento de tópicos, a 'incorporação perfeita' da produção de informações e o 'link contínuo' da disseminação de informações podem efetivamente alcançar o impacto 'inconsciente sobre o público'" (Wenling; Jiali, 2023, s.p., tradução nossa)[22].

Os autores do artigo descrevem quatro principais ações de confronto cognitivo nas redes sociais para gerar um impacto significativo ou mesmo decisivo na "guerra real": perturbações da informação, por meio da publicação de mensagens para influenciar a percepção do público sobre eventos; competição discursiva, com a divulgação de indicadores-chave de avaliação para

---

*22**社交媒体在**议题策划上的"**无形操控**"、**信息制作的"无痕嵌入"**、**信息**传播方式上的"**无缝链接**"，**能够有效达成对受众"无感入心"的影响***

construir um ambiente de discurso favorável e moldar a estrutura cognitiva; perturbação da opinião pública, que envolve ações específicas fora das redes sociais, mas em coordenação com divulgação *online*, para influenciar o público de forma sobre determinados assuntos; e o bloqueio de informações, que busca desequilibrar a competição cognitiva ao limitar a capacidade do adversário de se comunicar e influenciar, enquanto fortalece a posição do agressor no campo da informação e da narrativa (Wenling; Jiali, 2023).

Um estudo da RAND Corporation destaca que, após a reestruturação do ELP em 2015, o emprego de campanhas de desinformação nas redes sociais aumentou significativamente, com o estabelecimento da Força Estratégica de Apoio do Exército de Libertação Popular (PLASSF). Esse novo serviço dedicado à guerra de informação, utiliza estratégias para influenciar as Forças Armadas de Taiwan, a sociedade taiwanesa e políticos-chave com desinformação disseminada em plataformas como WeChat, Facebook, LINE[23] e o Professional Technology Temple (PTT) – fórum online popular de Taiwan utilizado para debates políticos e sociais. Há indicativos do uso de Taiwan pelo governo chinês como campo de teste e laboratório para avaliar a eficácia das campanhas de desinformação e refinar suas estratégias antes de expandi-las para outras regiões ou alvos. Além disso, a PLASSF, juntamente com outros órgãos chineses, foi acusada de manipulação das redes sociais durante as eleições de Taiwan em novembro de 2018, interferindo na democracia taiwanesa com desinformação e notícias falsas direcionadas a veículos de mídia, programas de rádio e televisão, e sites em Taiwan (Harold; Beauchamp-Mustafaga; Hornung, 2021; Applebaum, 2022).

De acordo com Zhang (2021), a China tem demonstrado uma presença ativa no emprego da desinformação como parte de seus esforços para influenciar Taiwan em direção à reunificação. Isso inclui um investimento significativo nas redes sociais, com páginas com grande número de seguidores passando a adotar repentinamente o chinês simplificado. Essa mudança é uma tentativa de normalizar e reforçar a presença cultural e política da China continental onde o idioma é utilizado, contribuindo ativamente para a disseminação viral da desinformação promovida por Pequim.

O uso de campanhas de desinformação nas redes sociais pela China não apenas reflete uma estratégia de guerra de informação bem definida, mas também revela uma compreensão sofisticada do poder da manipulação da narrativa e da influência psicológica. Através da reestruturação militar do ELP e do estabelecimento da PLASSF, a China demonstrou um

[23] Plataforma de mensagens instantâneas e redes sociais muito popular no Japão e Taiwan. Ela oferece recursos de mensagens privadas, grupos de discussão, chamadas de voz e vídeo, e integração com outros serviços, como pagamentos e compras on-line.

compromisso consistente em explorar as vulnerabilidades dos adversários, utilizando plataformas digitais para minar a coesão e o moral dos adversários (Zhang, 2021).

Em 19 de abril de 2024, a PLASSF foi dissolvida e dividida em três ramos independentes: a Força Aeroespacial do Exército de Libertação Popular, a Força Cibernética do Exército de Libertação Popular e a Força de Apoio à Informação do Exército de Libertação Popular. Essa modificação foi realizada para aprimorar a coordenação e o compartilhamento de informações entre os diferentes ramos do exército chinês e atingir a próxima ambição significativa do ELP, que é construir uma força de combate inteligente (Nouwens, 2024).

O foco em Taiwan como campo de teste e laboratório para refinar essas estratégias ressalta a intenção de Pequim de influenciar ativamente a política e a sociedade da ilha, inclusive durante processos democráticos. Essa abordagem não só levanta preocupações sobre a integridade dos processos democráticos, mas também destaca a importância crescente da segurança cibernética e da literacia digital na defesa contra ameaças dessa natureza (Harold; Beauchamp-Mustafaga; Hornung, 2021).

3.4 ESTUDO EX-POST FACTO SOBRE AS ESTRATÉGIAS DIGITAIS DA CAMBRIDGE ANALYTICA

3.4.1 Contextualização dos fatos

A Cambridge Analytica (CA), uma consultoria britânica especializada em perfil psicográfico e estratégias de marketing político, ficou notoriamente conhecida por seu envolvimento em uma série de atividades de manipulação de dados em diversos países. Suas práticas incluíam uma tecnologia proprietária de microsegmentação comportamental que utilizava a coleta massiva de informações pessoais de usuários de redes sociais sem consentimento explícito, com o objetivo de criar perfis detalhados para influenciar comportamentos políticos e eleitorais. Essas atividades levantaram sérias preocupações sobre privacidade e ética, resultando em repercussões legais e debates sobre regulamentações mais rígidas para proteger a integridade dos dados e a transparência nas campanhas políticas, como a dos Estados Unidos em 2016 (Isaak; Hanna, 2018).

De acordo com Kaiser (2020), uma *whistleblower* (denunciante) e ex-funcionária da Cambridge Analytica, a divulgação da participação da empresa nas eleições presidenciais dos Estados Unidos despertou um alerta sobre uma nova forma de conflito: a guerra orientada por dados *(Data-Driven Warfare).* Essa abordagem emprega o uso estratégico e tático de dados e

tecnologias de informação no contexto militar e de defesa. A *Data-Driven Warfare* envolve a coleta massiva de dados, análise avançada e aplicação de algoritmos para influenciar e manipular comportamentos e decisões em larga escala. No caso de Cambridge Analytica, isso incluía o uso de dados de 87 milhões de usuários do Facebook para criar perfis detalhados de eleitores, permitindo a segmentação precisa de mensagens políticas e anúncios, moldando assim o cenário político e eleitoral de maneira inédita e potencialmente disruptiva (Pijpers; Voskuijl; Beere, 2022).

A microsegmentação de eleitores possibilitou campanhas altamente direcionadas e persuasivas em favor do então candidato Donald Trump. Esse evento ressalta a importância cada vez maior atribuída aos algoritmos, *big data, machine learning* e outros ferramentas na modelagem do futuro das operações de guerra, demonstrando que, no contexto da era da informação, aqueles com maior acesso e habilidade para manipular dados possuem uma vantagem significativa (Erbschloe, 2017).

Segundo Wakefield (2019), embora as revelações de Kaiser sobre as práticas da Cambridge Analytica sejam consideradas significativas, suas motivações não são claras. Alguns consideram as informações controversas, pois só foram feitas após seu envolvimento ter sido revelado. O professor David Carroll, especialista em privacidade de dados e figura destacada no documentário "O Grande Hack", vê Kaiser como uma peça fundamental na narrativa histórica, mas sugere que ela pode estar omitindo detalhes determinantes em seu livro para preservar sua reputação e a de seus associados.

As investigações conduzidas pelas jornalistas do *The Guardian*, Carole Cadwalladr e Emma Graham-Harrison (2018), foram pioneiras ao desvendar a intricada rede de manipulação de dados associada à estratégia coordenada de um ator não estatal para eleição de Donald Trump. De acordo com suas descobertas, as atividades da Cambridge Analytica revelaram uma forma emergente de guerra informacional, descrita como “a ferramenta de guerra psicológica de Steve Bannon”.

Bannon, que ocupava o cargo de presidente executivo da rede de notícias *Breitbart News,* no Reino Unido, se associou a Robert Mercer – um bilionário estadunidense, fundador do comitê republicano *Make America Number 1* e investidor da Cambridge Analytica –, e a Alexander Nix –, então diretor da empresa privada de pesquisa comportamental e comunicação estratégica *Strategic Communication Laboratories Group (SCL).* A SCL surgiu do *Behavioural Dynamics Institute (BDI),* um consórcio formado por cerca de 60 instituições acadêmicas e centenas de psicólogos (Kaiser, 2020). Juntos, decidiram unir *Big Data* e redes sociais na metodologia militar de guerra de informação, e utilizá-la nas eleições dos Estados

Unidos por meio da CA. Foi então que Bannon assumiu o lugar de principal estrategista de Trump, enquanto a SCL, matriz da Cambridge Analytica, havia firmado contratos com o Departamento de Estado dos EUA e ampliado suas operações no Pentágono.

Cadwalladr e Graham-Harrison (2018) explicam que, além de influenciarem os resultados das eleições estadunidenses, Bannon e a CA também desempenharam um papel importante na campanha *Leave.EU* durante o processo de saída do Reino Unido da União Europeia. O *Brexit,* como ficou conhecido o movimento, passou por uma intensa estratégia de desinformação nas redes sociais, o que levou o parlamento britânico a criar um comitê para investigar a influência das *fake news* sobre o pleito.

A SCL contratou a Aggregate IQ, uma empresa canadense de desenvolvimento de software e de publicidade digital, para criar o Ripon, uma ferramenta de gerenciamento de relacionamento com clientes políticos. O sistema consistia em:

> uma coleção de aplicativos sofisticados, programas de gestão de dados, rastreadores de publicidade e bancos de dados, os quais, em conjunto, poderiam ser empregados para alcançar e influenciar indivíduos através de uma variedade de métodos, incluindo chamadas telefônicas automatizadas, e-mails, sites políticos, pesquisas voluntárias e anúncios no Facebook (House of Commons, 2019, p. 46, tradução nossa)[24].

No centro desse ecossistema, o Grupo SCL e sua subsidiária Cambridge Analytica desempenharam papéis determinantes na coleta e análise de dados. Aleksandr Kogan, um pesquisador da Universidade de Cambridge, havia desenvolvido um aplicativo de teste de personalidade chamado *This is your digital life,* que coletava dados de usuários do Facebook para traçar um perfil psicométrico. Baseado na psicologia comportamental, esse sistema era capaz de identificar a possível orientação política do usuário, o que levou a CA a adquirir o aplicativo do Kogan. Quando os usuários do Facebook participavam do experimento, eles acabavam fornecendo à Cambridge Analytica não apenas suas informações, mas também os dados de todos os amigos que os seguiam em seus perfis, possibilitando que a empresa tivesse acesso a um volume massivo de dados pessoais de cerca de 85 milhões de usuários (Solon, 2018).

Utilizando técnicas avançadas de manipulação de informações, essa sofisticada estratégia envolveu uma rede de relacionamentos corporativos que deu sustento ao esquema de

---

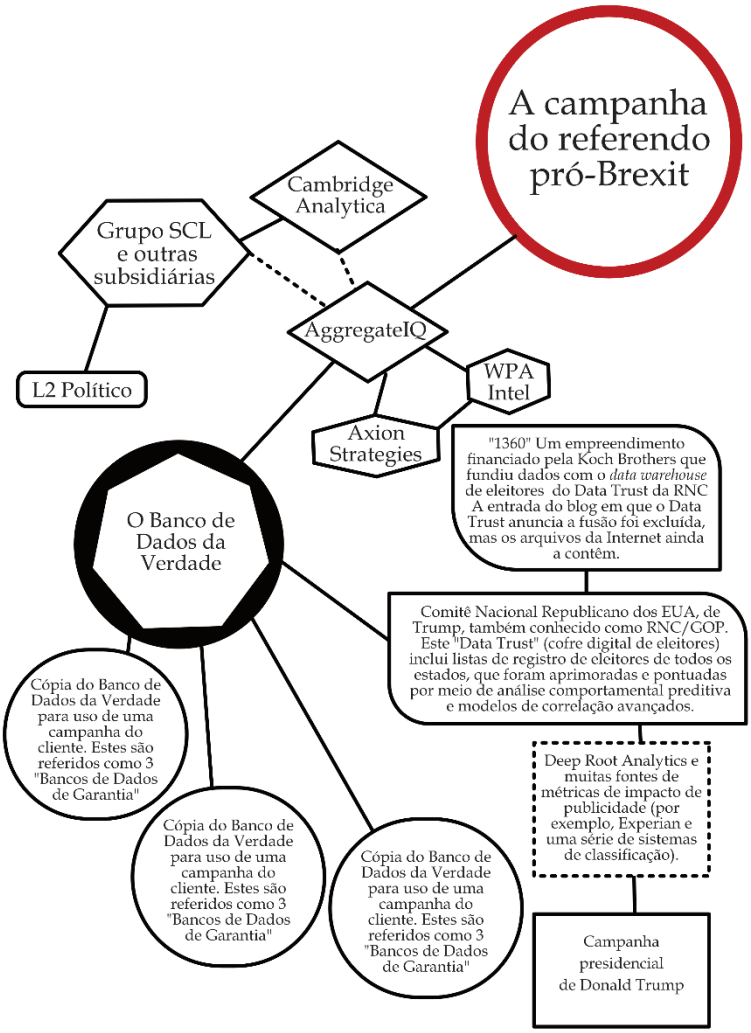
[24] *"This repository is a set of sophisticated applications, data management programs, advertising trackers, and information databases that collectively could be used to target and influence individuals through a variety of methods, including automated phone calls, emails, political websites, volunteer canvassing, and Facebook ads"*

direcionamento de mensagens e publicidades. A dinâmica demonstra como várias entidades colaboraram para coletar, analisar e utilizar dados eleitorais com o objetivo de influenciar campanhas políticas (House of Commons, 2019).

As informações básicas sobre eleitores eram concentradas em um banco de dados principal, replicado em três *backups*. As empresas envolvidas analisavam esses dados para desenvolver estratégias de segmentação e implementar as campanhas. O impacto das ações era mensurado permanentemente para ajustar as estratégias conforme necessário. Esse sistema ilustra um ecossistema sofisticado de manipulação de dados para campanhas políticas modernas, capaz de influenciar a opinião pública em escala global (House of Commons, 2019).

A Figura 2 fornece uma visão detalhada da interconexão entre várias entidades e campanhas políticas, destacando o contexto da campanha do referendo pró-Brexit e a campanha presidencial de Donald Trump.

Figura 2 - Rede de influência: a campanha do referendo pró-Brexit



Fonte: House of Commons (2019, p. 47, tradução nossa).

Os eventos das eleições dos Estados Unidos e o desligamento do Reino Unido da União Europeia (UE) foram os casos mais emblemáticos de disputa política que marcaram a história das redes sociais como divisores de águas, servindo como ponto de reflexão sobre os riscos associados ao uso indevido de dados pessoais e à manipulação digital em processos eleitorais. Ambos levantaram preocupações profundas sobre a privacidade dos usuários e a integridade dos sistemas democráticos, motivando Estados a desenvolverem mecanismos de regulação e transparência no ambiente digital (Isaak; Hanna, 2018; Webb; Dowling; Farina, 2021).

Kaiser (2018) defende que, além do *Brexit* e da vitória de Donald Trump, a Cambridge Analytica desencadeou ocorrências inesperadas, como o fortalecimento do fascismo e da extrema direita. A disseminação de *fake news* e de mensagens que difamavam de forma agressiva os adversários políticos foi fundamental para essa configuração. Com isso, as divisões sociais e políticas se intensificaram, alimentando de maneira significativa a polarização social e a desconfiança nas instituições. A manipulação da narrativa nas redes sociais teve um impacto profundo na sociedade, colocando em dúvida a integridade dos processos eleitorais e ameaçando os fundamentos da democracia.

Magallón (2019, *apud* Gobierno de España, 2022, p.198, tradução nossa)[25] faz um alerta sobre as origens, atores e objetivos das manipulações cognitivas por trás dessas campanhas de desinformação políticas: "a motivação ideológica ou puramente eleitoral tem a intenção de influenciar o resultado do processo. Geralmente têm origem na ação de partidos políticos ou de seus ambientes, embora às vezes possam contar com a ajuda de atores externos". Ele enfatiza que essas campanhas são mais difíceis de se sujeitar à legislação eleitoral devido à sua natureza complexa e muitas vezes transfronteiriça, tornando desafiador o controle e a aplicação de regulamentações específicas relacionadas a campanhas eleitorais. O autor complementa que há um modelo de negócios priorizado pela questão econômica que explora a tensão eleitoral. No caso das eleições estadunidenses, esse modelo pode ser evidenciado pela contaminação do debate público originada nas fazendas de conteúdo da Macedônia, na Península dos Bálcans, Sudeste da Europa (Subramanian, 2017).

A cidade de Veles, na Macedônia, passou a ser o epicentro da criação e disseminação de notícias falsas na campanha de Trump, especialmente através das redes sociais, com *hoaxes* (notícias falsas sensacionalistas). Hughes e Waismel-Manor (2020) revelam essas mensagens geraram mais engajamento no Facebook do que conteúdos de grandes veículos de notícias como

---

[25] *"La motivación ideológica o puramente electoral pretende incidir en el resultado del proceso. Suelen tener su origen en la acción de los partidos políticos o sus entornos, aunque en ocasiones puedan contar con la ayuda de actores externos".*

os jornais *New York Times* e o *Washington Post*. Muitas dessas histórias falsas, como a alegação de que Hillary Clinton vendeu armas para o grupo extremista ISIS e que o Papa Francisco endossou a candidatura de Donald Trump, originaram-se de sites com IP apontando para Veles.

Subramanian (2017, *apud* Gobierno de España, 2022) destaca que Boris – nome fictício um jovem de 18 anos de Vales –, começou despretensiosamente a compartilhar informações falsas em suas próprias páginas de internet e redes sociais, visando lucrar através da monetização nas redes. Ele ficou surpreso ao ver que sua publicação com uma notícia sensacionalista sobre Donald Trump teve grande repercussão, rendendo algum dinheiro com anúncios do Google AdSense. Entre agosto e novembro de 2016, Boris obteve quase US$ 16 mil através de seus dois sites em apoio a Trump, o que foi considerada uma boa quantia ao ser comparada a um salário médio mensal da Macedônia de US$ 371. Os resultados levaram outros jovens de sua cidade a se envolveram na prática e passaram a criar e divulgar notícias falsas para obter ganhos financeiros através de anúncios online.

Allcott e Gentzkow (2017) explicam que a motivação financeira é uma das principais motivações por trás da disseminação intencional de notícias falsas. Isso porque as notícias que se tornam virais nas redes sociais têm o potencial de gerar receita significativa por meio de publicidade quando os usuários acessam o site original. A segunda motivação é ideológica, já que alguns disseminadores de *fake news* buscam promover candidatos ou causas que apoiam.

Um estudo realizado pelo Instituto de Tecnologia de Massachusetts (MIT, na sigla em inglês) em 2018, revelou que as notícias falsas possuem um alcance de audiência seis vezes maior em comparação às notícias verdadeiras. A busca por ser o primeiro a divulgar uma informação é um dos motivos que impulsiona os indivíduos a contribuir para a disseminação de notícias enganosas. Além do mais, a capacidade das notícias falsas de provocar surpresa e serem percebidas como conteúdo novo e valioso desperta o interesse das pessoas e as motiva a compartilhar essas informações com sua rede de contatos, impulsionando ainda mais sua propagação.

O caso da fazenda de *fake news* da Macedônica representa um desafio considerável para a integridade dos processos eleitorais e das informações disseminadas nas redes sociais. Além disso, ressalta a necessidade do combate à propagação da desinformação e de promover a educação midiática para fortalecer a resiliência das sociedades diante de campanhas de manipulação da informação (Hughes; Waismel-Manor, 2020).

3.4.2 Tecnologia persuasiva e operações de influência

Para exercer suas operações de influência entre os usuários do Facebook, a Cambridge Analytica desenvolveu um método de análise psicográfica denominado Ocean. O nome é um acrônimo dos cinco perfis psicológicos definidos pela empresa: *openness* (abertura a novas experiências), *conscientiousness* (consciência), *extroversion* (extroversão), *agreeableness* (amabilidade) e *neuroticism* (neuroticismo). Esses perfis foram utilizados para identificar e categorizar o público-alvo com a finalidade de direcionar campanhas e anúncios políticos personalizados. O método permitia à CA segmentar os usuários e adaptar suas mensagens políticas com o intuito de influenciar suas decisões e comportamentos eleitorais (Isaak, 2018; Kaiser, 2020).

Ao combinar dados geográficos, demográficos e psicográficos, como traços de personalidade e intenção de voto, a Cambridge Analytica pôde criar uma visão granular e altamente direcionada dos eleitores efetivos e potenciais. Os dados usados para essas análises eram coletados de várias fontes, como de parceiros de clientes, fornecedores comerciais, pesquisas qualitativas/quantitativas diretas e redes sociais, principalmente do Facebook (Amer; Noujaim, 2019), para revelar tendências ocultas de eleitores e gatilhos comportamentais. Os dados eram coletados da rede por meio do aplicativo *"thisisyourdigitallife"*. Nesse método de *microtargeting*, o eleitor era tratado como um consumidor. O investimento em propaganda destinado a cada usuário variava conforme seu nível de influência e receptividade às sugestões inferidas de seu perfil (Kaiser, 2020).

A psicometria avançada empregada pela Cambridge Analytica durante a campanha presidencial dos Estados Unidos em 2016 exemplifica essa complexa interseção entre tecnologia persuasiva, política e privacidade de dados. Esse caso ilustra não apenas o poder crescente das análises de dados na esfera política, mas também as implicações éticas e políticas associadas à coleta e manipulação de informações pessoais em larga escala. A influência desses sistemas de controle de dados em eventos políticos de grande porte ressalta a necessidade de uma reflexão crítica sobre o uso ético e transparente das tecnologias de análise de dados e seus impactos na democracia e na sociedade em geral (Rehman, 2019).

Informações de um catálogo promocional da Cambridge Analytica (2016) revelam que a empresa usava grandes quantidades de dados, incluindo consumo, estilo de vida, censo e histórico de votação, para compreender os elementos psicológicos subjacentes motivadores do voto para cada segmento-alvo a fim de construir perfis avançados de eleitores individuais. Esses perfis também englobavam informações detalhadas sobre a probabilidade de um público-alvo

comparecer às urnas, seu grau de persuasibilidade e as questões que lhes eram mais importantes. Tais segmentações ofereciam às campanhas um retrato abrangente dos grupos-alvo, permitindo uma compreensão mais profunda dos apoiadores tradicionais, além de identificar e estabelecer conexão com novos. Os especialistas em mensagens políticas da CA auxiliavam as campanhas na criação de mensagens que eram dirigidas diretamente aos eleitores-alvo, facilitando a formação de uma conexão com os apoiadores e gerando resultados eleitorais eficazes. A empresa ostentava uma experiência de 25 anos na "vanguarda da mudança comportamental e recursos tecnológicos de ponta" (p. 3, tradução nossa)[26].

Segundo Rêgo e Barbosa (2020), o publicitário brasileiro André Torreta, foi um representante da empresa no Brasil por meio da SCL. Ele decidiu se juntar à CA após ser apresentado pela consultoria ao método Ocean ainda durante a campanha eleitoral de Trump. Nessa época, os estrategistas da CA estavam interessados nas eleições brasileiras de 2018. Ainda segundo as autoras, Torreta revelou que chegou a realizar três campanhas naquele ano, incluindo a do governador do Amapá (PA), Waldez Góes.

O publicitário, que anteriormente havia participado das campanhas de Fernando Henrique Cardoso, José Sarney e Roseana Sarney, observou que, nos Estados Unidos, a Cambridge Analytica operava com grande precisão, pois possuía, em média, cerca de 7 mil dados sobre cada indivíduo pesquisado. Por outro lado, no Brasil, a situação era diferente, pois os bancos de dados sobre os cidadãos ainda estavam em processo de formação. Além disso, as leis brasileiras eram mais rigorosas que as dos Estados Unidos. No entanto, mesmo assim, já em 2017, era possível acessar rapidamente cerca de setecentas informações sobre cada cidadão brasileiro pesquisado (Rêgo; Barbosa, 2020).

Após realizar essa análise exemplificativa sobre o emprego da guerra cognitiva por parte da Rússia, China e Cambridge Analytica, foi possível constatar que agentes estatais e não-estatais têm utilizado táticas altamente sofisticadas para influenciar e manipular percepções, utilizando a psicologia social e a disseminação de informações nas redes sociais como estratégias. Esta confirmação é importante pois revela as questões fundamentais sobre as ameaças à segurança e à soberania nacional a que os Estados estão sujeitos.

Refletindo sobre os fatores que podem estar em jogo, cabe ressaltar que o Brasil, sendo o quinto maior país do mundo em extensão territorial[27], com uma rica biodiversidade, recursos naturais e energéticos abundantes, incluindo um mercado consumidor em constante crescimento, tem se tornado um ponto de atração para os interesses de inúmeras nações. Em

---

[26] *"the forefront of behavioral change and cutting edge technological capabilities"*
[27] *IBGE (2023).*

seu pronunciamento na cúpula do G7 em 2019, o presidente da França, Emmanuel Macron, deixou claro as intenções na Amazônia, considerando-a como “um bem comum", um “tesouro de biodiversidade”, tendo, inclusive, sugerindo a necessidade de se discutir a elaboração de um “estatuto internacional” ao pedir a “mobilização de todas as potências” para combater o desmatamento e investir no reflorestamento da região (Amorim, 2021).

Os posicionamentos de Macron sobre a importância ambiental e climática da Amazônia elevam a questão ambiental amazônica a um nível de segurança global, o que já vinha sendo apontado por Buzan e Waever (2003) em relação aos movimentos dos Estados Unidos sobre a mesma pauta. Os autores afirmam que a securitização ambiental é vista como um ponto de tensão nas relações entre o Brasil e outros atores internacionais, como os EUA e organizações ambientais, assim como o papel de liderança do país nas dinâmicas de segurança da América do Sul. Neste contexto, a guerra cognitiva representa um desafio importante para a percepção pública sobre questões complexas como temas ambientais e geopolíticos.

Uma pesquisa realizada pelo Statista[28] sobre o ecossistema de usuários de internet no Brasil revela de forma significativa a importância das redes sociais na realidade cotidiana da população brasileira. Com 177 milhões de usuários digitais, representando uma taxa de inclusão digital de 81,79%, o país aparece como a quinta maior população digital do mundo. Isso significa que, a cada 100 brasileiros, 82 estão conectados à internet, o que representa 94% desse universo. Além disso, 175 milhões de pessoas têm acesso à rede móvel, destacando a disseminação das tecnologias de informação e comunicação entre a população (Bianchi, 2024).

Um outro fator relevante é que o mercado de influenciadores dinamizou o ambiente das redes sociais, atraindo cada vez mais atenção e investimentos. Enquanto as plataformas digitais disputam seu espaço nesse terreno fértil, a atenção e o tempo dos usuários se tornam elementos valiosos. Paralelamente, o discurso político brasileiro, marcado por intensos debates e profunda polarização, cresce fortemente no ecossistema digital, adicionando uma camada de complexidade ao cenário (Bianchi, 2024).

Nesse contexto, o WhatsApp se destaca como a principal plataforma de mensagens instantâneas, presente em praticamente todos os aparelhos celulares do país. Com a integração de pagamentos móveis e comércio social, o aplicativo está perto de se consolidar como uma super ferramenta social, ampliando sua relevância no ecossistema digital brasileiro. À medida que o uso da internet se expande, a competição por plataformas interativas de mensagem

[28] Banco de dados abrangente com mais de 1 milhão de fatos e estatísticas em 170 setores e mais de 150 países.

também cresce em todos os aspectos, buscando extrair o máximo da atenção dos usuários na esfera online do país (Bianchi, 2024).

Compreender e responder eficazmente às dinâmicas da guerra cognitiva em curso torna-se, portanto, fundamental para proteger os interesses nacionais e preservar a estabilidade política e social do Brasil. Isso envolve a análise de como as diversas forças políticas, sociais e econômicas interagem por meio das redes sociais e influenciam o exercício do poder por meio da Expressão Psicossocial do Poder Nacional. Este desafio requer uma abordagem contínua e adaptável para enfrentar as evoluções constantes nesse campo complexo, conforme será abordado no próximo capítulo. A análise crítica e a reflexão sobre essas questões são componentes importantes para a formulação de políticas eficazes que protejam os pilares fundamentais da nação brasileira e fortaleçam sua resiliência frente às ameaças contemporâneas à sua estabilidade e soberania.

3.5 ANÁLISE COMPARATIVA DOS ESTUDOS EX-POST FACTO

Ao analisar os casos da Rússia, China e Cambridge Analytica, é possível extrair lições importantes para compreender e enfrentar os desafios da guerra cognitiva nas redes sociais e sua influência na Expressão Psicossocial do Poder Nacional brasileiro. Esses casos demonstram como campanhas coordenadas de desinformação podem ser utilizadas para semear discórdia, polarizar a opinião pública e enfraquecer a coesão social. A Rússia, por exemplo, tem utilizado técnicas avançadas de ciberespionagem e propaganda para interferir em processos eleitorais de outros países (Soldatov; Borogan, 2015), enquanto a China investe em tecnologia e controle de informação para moldar narrativas favoráveis aos seus interesses (Zhang, 2021). A Cambridge Analytica mostrou como dados pessoais podem ser explorados para segmentar e influenciar grupos específicos de eleitores, alterando resultados políticos (Erbschloe, 2017).

Estudar métodos antigos de guerra cognitiva, como a "Maskirovka" russa e as obras de Sun Tzu, mostra como essas estratégias mudaram ao longo do tempo. Isso ressalta a importância de preparar o país para as ameaças contemporâneas. Essas práticas sugerem uma abordagem que leve em conta tanto os desafios atuais quanto as lições do passado. Assim, é possível fortalecer a nação contra manipulações e interferências externas, especialmente nas redes sociais, que têm se tornado um campo fértil para a disseminação de desinformação e influências maliciosas.

Esses casos revelam a complexidade das estratégias utilizadas nas redes sociais, que vão desde a criação de narrativas enviesadas até a disseminação massiva de desinformação com o

intuito de moldar a opinião pública. A utilização da psicologia social como ferramenta para explorar vulnerabilidades emocionais e cognitivas dos usuários, aliada à disseminação estratégica de informações, destaca o empenho na busca pela sofisticação de ferramentas e mecanismos que sejam mais eficientes e sutis. A compreensão do domínio cognitivo como novo campo de batalha destaca a importância de uma abordagem proativa na proteção da soberania nacional. A sofisticação das táticas empregadas por esses atores estatais e não-estatais para influenciar e manipular percepções transcendem fronteiras geográficas e políticas, englobando inclusive o Brasil, conforme informam Bradshaw, Bailey e Howard (2021) na pesquisa do Oxford Internet Institute (OII).

O estudo do OII destaca a posição do Brasil no contexto da guerra cognitiva global e aponta o país como um dos participantes ativos na propagação de informações falsas e enganosas pelas redes sociais. A estratégia de utilizar tropas cibernéticas por meio do recrutamento de membros é uma manobra para que os agentes maliciosos possam agir em tempo integral com o objetivo de controlar o espaço de informação. Além de coordenar os ataques, essas equipes também utilizam uma variedade de ferramentas e métodos de manipulação nas redes sociais, incluindo a realização de operações de influência no exterior. O envolvimento brasileiro revela a intencionalidade operativa como parte ativa, ao mesmo tempo que evidencia a vulnerabilidade diante de ações externas.

A realidade apresentada expõe os desafios que a guerra cognitiva nas redes sociais representa para o Brasil. A disseminação da desinformação e a manipulação da opinião pública online se apresentam como ameaças à segurança nacional, à coesão social e à projeção internacional do país. Essa preocupação é destacada na mensagem presidencial enviada ao Congresso Nacional sobre o Plano Plurianual 2024-2027 (Brasil, 2023e). O documento enfatiza a erosão da coesão social e a polarização da sociedade como um dos dez principais riscos globais, e realça os riscos à democracia associados ao aumento da vulnerabilidade da segurança de dados devido à digitalização da sociedade:

> Soma-se a isso a preocupação com a propagação massiva de desinformação e *fake news*, com implicações político-sociais. Esse é mais um canal para alimentar o fenômeno de polarização crescente da sociedade e de erosão da coesão social, que fomenta o risco para a democracia no mundo (Brasil, 2023e, p. 57).

Agrega-se a essas discussões, a pesquisa sobre o ecossistema de usuários de internet no Brasil, que expõe a relevância das redes sociais como parte integrante da vida cotidiana da

população, destacando a profunda influência dessas plataformas na sociedade contemporânea (Bianchi, 2024). Conforme indicam os estudos, o país se posiciona como a quinta maior população online do mundo, impulsionada pelo crescente acesso à internet móvel (Bianchi, 2024).

As redes sociais são um tema central na internet no Brasil. A popularidade dessas plataformas impulsiona tanto o mercado de influenciadores quanto a discussão política online. Outra característica dessa realidade digital brasileira é o envio de mensagens instantâneas, que se tornou uma das principais atividades entre os usuários de aplicativos móveis. Um exemplo da relevância desses programas é o WhatsApp, extremamente popular e presente em quase todos os smartphones no país, que está evoluindo além de seu uso original de mensagens rápidas e se transformando em um "super aplicativo" ao incorporar novas funcionalidades, como pagamentos móveis e social commerce (Bianchi, 2024).

As redes sociais possuem uma grande influência na sociedade brasileira, e, por esta razão, o entendimento de seu funcionamento se faz cada vez mais necessário para a detecção e combate a possíveis ameaças. A disseminação de informação, a interação social e a formação de opinião são fatores que cada vez mais necessitam de políticas públicas para garantir a soberania e estabilidade do país contra os riscos evidenciados. A crescente dependência, integração e diversidade das redes sociais expõem o Poder Nacional a um espectro amplo de ameaças. A capacidade de atores externos moldar a opinião pública, conforme demonstrado nos estudos *ex-post facto*, ressalta a importância de redobrar os esforços de proteção do país contra influências e manipulações. A desinformação tem demonstrado o poder de distorcer debates políticos, polarizar a sociedade e fragilizar a confiança nas instituições, representando riscos significativos para a segurança nacional. Esses desafios tornam-se cada vez mais complexos em um ambiente digital altamente interconectado, exigindo estratégias robustas para proteger a soberania e a estabilidade do Brasil (Congresso Nacional, 2023).

A manipulação das vulnerabilidades psicológicas e cognitivas dos usuários por agentes governamentais e não-governamentais apresenta uma ameaça substancial à estabilidade e à segurança nacional. A crescente sofisticação dessas táticas evidencia a urgência de uma abordagem multidisciplinar, que deve incluir a colaboração entre o governo, o setor privado e a sociedade civil, com o objetivo de proteger a Expressão Psicossocial do Poder Nacional e reforçar a segurança cibernética diante dos desafios impostos pela era digital.

4 AS AMEAÇAS À EXPRESSÃO PSICOSSOCIAL DO PODER NACIONAL

4.1 A FENOMENOLOGIA DA GUERRA E SUA ORIGEM SOCIOLÓGICA

Visacro (2018, p. 20) aponta que “antes de ser um fenômeno político, a guerra é um fenômeno social”, ressaltando a influência das sociedades na origem dos conflitos armados e não como ação unicamente dos exércitos, líderes militares ou políticos. Complementando essa ideia, Howard (1984), em “*The Causes of Wars*”, enfatiza que a guerra está intimamente ligada às dinâmicas culturais, econômicas e históricas das sociedades. Ele defende que, para entender as causas das guerras, é necessário analisar contextos sociais mais amplos, indo além das decisões políticas ou militares.

Vicente Fisas (2004) reforça a perspectiva de que o conflito é mais do que simplesmente violência, sendo uma interação social complexamente moldada por diversas variáveis dinâmicas entre indivíduos opostos ou discordantes. Essa interação pode levar tanto a consequências benéficas, como debates construtivos e mudanças sociais. quanto a impactos prejudiciais. como sofrimento ou desolação. Essa dualidade intrínseca ao conflito possibilita sua gestão internamente pelas partes envolvidas, com ou sem interferência externa. Os valores culturais e as crenças moldam fortemente essa construção social através de influências como instintos e emoções, afetando atitudes e comportamentos.

Ao considerarmos a visão de Visacro (2018), Howard (1984) e Fisas (2004), é possível perceber que a origem dos conflitos está profundamente enraizada nas interações sociais, nas estruturas de poder e nas relações entre diferentes grupos dentro de uma sociedade. Essas perspectivas ressaltam a importância de compreender as dinâmicas sociais subjacentes a esse fenômeno socialmente construído, indo além da mera análise dos aspectos político-militares.

Neste contexto, a compreensão da guerra como um fenômeno social impõe um estudo mais amplo das relações de poder e das dinâmicas que levam à produção dos conflitos nas redes sociais. Essa realidade evidencia a necessidade de se compreender como a guerra cognitiva no ambiente online afeta a Expressão Psicossocial do Poder Nacional, e como os aspectos socioculturais, psicológicos e comportamentais da população influenciam e são influenciados por ela.

Sob esse aspecto, a análise anterior dos elementos, buscou identificar dados oportunos que forneçam uma compreensão mais robusta sobre essas dinâmicas do poder, a formação de alianças e coalizões, a construção de narrativas de legitimidade e a mobilização de recursos em

contextos de conflito nas redes sociais, que afetam ou possam impactar a Expressão Psicossocial do Poder Nacional brasileiro.

4.2 O PODER E SUAS DINÂMICAS NO CONTEXTO DA GUERRA COGNITIVA

O poder pode ser descrito como uma força complexa e em constante transformação. Essa força exerce influência sobre as relações sociais e políticas em variados níveis. Com essa perspectiva, Lukes (1974) destaca a importância das estruturas sociais e dos padrões culturais na determinação dos comportamentos e das escolhas individuais. Segundo o autor, o poder não se limita às ações e decisões visíveis; ele também está relacionado à capacidade de moldar o ambiente social e cultural no qual essas decisões ocorrem.

Sob esse ponto de vista, o autor explica que o poder pode ser compreendido a partir de três dimensões interdependentes: a primeira se refere aos processos de tomada de decisão; a segunda, à habilidade de controlar a agenda dessas decisões; e, por fim, a terceira dimensão diz respeito à capacidade de moldar as percepções e preferências das pessoas, muitas vezes de forma imperceptível. Essa configuração permite entender como o poder pode atuar de maneira sutil, influenciando como os indivíduos percebem a realidade e fazem suas escolhas.

Essa última dimensão, mais especificamente, opera no âmbito das convicções, valores e visões de mundo, fazendo com que os indivíduos ajam em concordância com os interesses daqueles que detêm o poder, muitas vezes sem perceberem essa influência. Ela é intensivamente explorada na guerra cognitiva. Os agentes envolvidos nessa guerra buscam influenciar as crenças, valores e visões de mundo dos usuários de forma sutil e complexa, utilizando estratégias como a disseminação de narrativas enviesadas, o uso de gatilhos emocionais e a criação de bolhas de filtro (Santaella, 2018).

Ao selecionar e apresentar narrativas enviesadas que se alinham aos interesses pretendidos, os agentes da guerra cognitiva podem influenciar as percepções e reforçar determinadas visões de mundo (Cluzel, 2020). Os gatilhos emocionais influenciam as ações ou posturas ideológicas dos usuários, modificando ou validando suas reações e comportamentos. Por conseguinte, as “bolhas de filtro” reforçam as crenças e visões de mundo ao expor os indivíduos constantemente a informações que corroboram essas perspectivas já existentes. Esse processo restringe a amplitude do pensamento e a capacidade de considerar outras perspectivas, aumentando a influência dos agentes de guerra cognitiva (DiRestra 2018).

A filosofia política de Rousseau (2013), presente em sua obra clássica “O Contrato Social”, oferece uma abordagem teórica valiosa para o entendimento de como funciona a

dinâmica da guerra cognitiva nas redes sociais. Rousseau acreditava que a soberania popular e o contrato social fundamentavam a autoridade legítima e o poder político. Para ele, em um estado democrático, o poder é legitimado pela vontade da maioria dos cidadãos, com o consentimento dos governados. Essa ideia representa o princípio da soberania popular.

Para Rousseau (2013), a origem do poder do Estado reside nas próprias pessoas, que se unem em sociedade, concordando em renunciar a uma parcela da sua liberdade em troca de proteção e segurança estatal. No entanto, a autoridade do Estado deve ser compreendida não como um poder arbitrário ou simplesmente repressor, mas como um instrumento para possibilitar o alcance de objetivos comuns. Tais objetivos podem variar em função da constituição, bem como das concepções fundamentais de cada sociedade. No caso do Brasil, esses objetivos coletivos estão previstos na Constituição Federal de 1988. É na Constituição que se consubstanciam os princípios estruturantes não negociáveis do Estado, como a promoção do bem-estar social, a salvaguarda dos direitos individuais e transindividuais, a busca permanente da justiça social e a perenidade do regime democrático (Brasil, 1988).

Em linha com essa perspectiva, Putnam (1992) elabora sua teoria com base no conceito de "capital social", cuja confiança é o fundamento para a coesão e o funcionamento eficiente das sociedades. Essa confiança recíproca entre os cidadãos, sejam eles integrantes de uma comunidade específica ou membros de uma nação, é o centro das relações interpessoais sólidas, que fortalece as instituições públicas, dinamiza o desenvolvimento econômico e mantém a coesão social. Esse clima de mútua crença propicia um ambiente favorável à colaboração entre os indivíduos, estimulando a livre expressão de pontos de vista, bem como uma participação cidadã ativa nos processos democráticos.

Já Castells (1999) aborda os desafios que a sociedade em rede traz para a coesão social, enfatizando a relevância da participação e do engajamento cívico na era digital. Ele defende que as novas tecnologias proporcionam oportunidades para uma participação mais ampla dos cidadãos na formulação de decisões políticas, por meio de plataformas de interação online e movimentos sociais digitais. É nesse processo de articulação de diversas correntes comunicativas que a esfera pública contemporânea se molda e se consolida. Para Castells, a internet é o centro dessa sociedade reticular, altamente conectada e interligada, atuando como a "espinha dorsal da comunicação global mediada por computadores" (p. 431).

No contexto da construção da confiança social e do funcionamento da sociedade, como discutido por Putnam (1992), e da transformação da democracia na era digital, como abordada por Castells (1999), o acesso ao ambiente virtual é o requisito fundamental para a legitimação do contrato social contemporâneo. É nesse novo espaço público que os cidadãos exercem sua

liberdade de expressão e participam do debate democrático, fornecendo uma nova perspectiva à teoria de Rousseau (2013). Com essa visão sobre a importância da internet para a participação cívica, a Organização das Nações Unidas (ONU, 2011) defende o acesso de todos à essa rede global virtual, postulando que a sua obstrução ou impedimento equivale a uma restrição ao direito à liberdade de expressão, violando o princípio estabelecido no Pacto Internacional de Direitos Civis e Políticos de 1966.

A ideia de contrato social de Rousseau (2013) encontra um paralelo importante com a dinâmica das redes sociais. O compartilhamento das informações e as interações online criam uma confiança semelhante a um contrato social digital. Mas essa tecnologia está mudando a relação existente entre o indivíduo e o Estado, que tem perdido seu poder hegemônico na sociedade. Com a internet, os cidadãos têm mais poder para influenciar e mudar estruturas sociais enraizadas, e mais possibilidade de se mobilizarem e revisarem o contrato social. Como resultado, as hierarquias tradicionais estão sendo questionadas e a voz do cidadão está sendo amplificada, como destacou Choucri (2012).

Joseph Nye Jr. (2012), um dos mais proeminentes teóricos do neoliberalismo no campo das relações internacionais, aborda o conceito de poder em termos tipológicos. Para ele, o poder não é um fenômeno isolado, devendo ser compreendido em suas várias formas. Desta forma, classifica o poder em diferentes categorias, como o *soft power* (poder brando), o *hard power* (poder duro) e o *smart power (*poder inteligente), sendo esta uma combinação das duas primeiras. Tal abordagem ajuda a compreender a dinâmica da influência e da decisão em contextos geopolíticos atuais.

A perspectiva de Nye Jr. para o *soft power* enfatiza que, "em termos simples, (o poder) é a capacidade de obter os resultados desejados e, se necessário, mudar o comportamento dos outros para obtê-los" (2002, p.30). Ele enfatiza a importância da atratividade e da persuasão como meios eficazes para influenciar a opinião pública e moldar percepções, fazendo com que uma determinada agenda, valores ou ideias sejam mais atraentes e desejáveis para outros atores. Estas propostas não apenas evidenciam a importância do poder na diplomacia e nas relações internacionais, como ainda permitem um paralelo com o exercício do domínio no contexto da guerra cognitiva empregada nas redes sociais. Nesse ambiente, o poder é exercido na construção e disseminação de narrativas para influenciar opiniões e receber apoio para ideias e causas diversas, gerando impactos significativos, tanto na política interna, como no ambiente internacional.

Naím (2014) traz uma nova perspectiva sobre o poder. Sua teoria sobre a globalização defende que, seja no âmbito político, empresarial ou mesmo em situações de conflito, o poder

está passando por uma significativa fragmentação decorrente de uma série de mudanças rápidas e substanciais, que têm provocado uma reconfiguração profunda nas dinâmicas globais. Nessa nova composição, potências tradicionais enfrentam desafios sem precedentes em suas esferas de influência. Ao mesmo tempo, novos atores emergem com formas inovadoras de exercer o poder ou contestar o que já está estabelecido. Nesse novo contexto, a evolução da tecnologia e a interconexão global exercem um papel central, contribuindo para a intensificação dessa fragmentação e tornando o ambiente do poder ainda mais complexo e imprevisível. Potências hegemônicas, como os Estados Unidos, estão encontrando crescentes limitações em sua capacidade de influência, bem como grandes corporações, que enfrentam uma crescente ameaça com a ascensão de empreendimentos menores.

Ao explicar essas transformações, Naím (2014) defende a ideia de que três revoluções estão mudando a natureza do poder, apresentando formas mais distribuídas, horizontalizadas e flexíveis. Segundo ele, essas revoluções são proporcionadas pelos avanços tecnológicos. São elas: a revolução da mobilidade, a revolução da cognição e a revolução da cooperação. A revolução da mobilidade se refere a novas formas de conecção e organização, facilitadas pelo acesso à informação e à mobilidade física e social. A revolução da cognição aborda a tomada de decisão mais informada e precisa devido à capacidade de processar e de analisar grandes quantidades de dados. Finalmente, a revolução da cooperação se refere à capacidade de colaborar e de trabalhar em conjunto, seja a distância ou de forma hierárquica, ainda que menos rígida, proporcionada por novos recursos tecnológicos.

As redes sociais abriram espaço para que grupos e indivíduos contestem as narrativas tradicionais e ampliem sua influência. Isso faz dessas plataformas ferramentas poderosas na fragmentação e descentralização do poder, trazendo desafios para que governos e instituições mantenham o controle e a autoridade. Segundo Naím (2014), essa nova dinâmica tem profundas implicações para a política e para a sociedade. De um lado, há uma maior diversidade de vozes e perspectivas, já que grupos antes marginalizados ou minoritários agora conseguem se expressar. Por outro, essa fragmentação pode gerar instabilidade, pois as instituições tradicionais muitas vezes encontram dificuldades para se adaptar e manter o controle diante dessa nova realidade.

O trabalho de Hans Morgenthau (2003) é um ponto de referência essencial para entender como o poder se distribui entre os Estados. A partir da teoria realista, o diplomata e acadêmico alemão introduziu o conceito de “balança de poder” como uma peça-chave para entender as complexas relações entre as nações. Para ele, essa balança é algo natural no cenário internacional, influenciando as ações e ambições de cada país. Funciona como uma espécie de

limitador, impedindo que as desigualdades de poder sejam extremas e garantindo que nenhum país domine os outros de forma absoluta.

No entanto, para que a balança de poder funcione de forma eficaz, é importante que os Estados a reconheçam e a aceitem como um ordenamento comum que norteia suas ações. Essa aceitação se traduz na busca por um equilíbrio de poder distribuído de forma relativamente homogênea, onde nenhuma nação detém supremacia absoluta (Morgenthau, 2003). Assim como na geopolítica, na guerra cognitiva nas redes sociais, o equilíbrio do poder se manifesta através da competição entre diversos atores digitais pela influência na opinião pública e controle da narrativa. Isso inclui governos, empresas, grupos de interesse e indivíduos que formam alianças, coalizões e confrontos online para promover agendas, combater a desinformação e manipular as plataformas digitais.

Essa pesquisa possibilitou identificar que, embora a guerra cognitiva nas redes sociais utilize ferramentas e estratégias diferentes daquelas empregadas no ambiente geopolítico tradicional, algumas das dinâmicas de poder subjacentes são as mesmas. Assim como nações disputam território e recursos, a competição na guerra cognitiva ocorre por meio do controle da narrativa e da percepção pública. A disseminação de notícias falsas, criação de perfis falsos e a utilização de *bots* buscam influenciar o comportamento e as crenças dos usuários, usando a influência como exercício do poder.

Na guerra cognitiva, a assimetria de poder é um fator determinante para se alcançar os objetivos, limitando a capacidade de grupos minoritários e indivíduos de se expressar e defender seus pontos de vista. Grandes empresas de tecnologia, governos e grupos de interesse possuem recursos e influência superiores, o que os coloca em vantagem na disputa pela narrativa online. A utilização de "fazendas de *trolls*" por agentes maliciosos, públicos ou privados, para espalhar propaganda e censurar a dissidência; a disseminação de teorias da conspiração por grupos extremistas em plataformas de rede social; e a manipulação de algoritmos por empresas para promover seus produtos e serviços são alguns dos exemplos em que a assimetria do poder se manifesta.

4.3 PRINCÍPIOS CONCEITUAIS SOBRE O PODER NACIONAL E SUA EXPRESSÃO PSICOSSOCIAL

A discussão conceitual sobre o Poder Nacional é um problema complexo de elevada dinâmica. O tema tem sido objeto de análise por diversos teóricos ao longo da história das Relações Internacionais. Como pôde ser observado, Morgenthau (2003) foi um dos autores que

mais contribuíram para esta discussão. Segundo ele, as dimensões do poder ultrapassam a mera acumulação de recursos militares ou econômicos. Ao argumentar que o poder é também a capacidade de influenciar e modelar o ambiente internacional de acordo com os objetivos de um Estado, ele expande o conceito de Poder Nacional para além do território, não limitando-o apenas a recursos físicos, mas incluindo também o potencial de influenciar o seu entorno e obter os resultados desejados globalmente.

A essência do Poder Nacional, de acordo com Morgenthau (2003), reside na força exercida por um grupo de indivíduos sobre as mentes e ações de outros. A população em geral, entretanto, tende a ser influenciada e controlada pelo poder estabelecido, se identificando emocionalmente com ele, em vez de exercer um papel ativo na definição desse poder. Para direcionar os impulsos individuais do poder, as sociedades estabelecem mecanismos de controle e, consequentemente, a maioria das pessoas se torna objeto do poder exercido por poucos.

Morgenthau (2003) também afirma que, quando um indivíduo percebe o poder de seu país, ela sente um orgulho compartilhado, como se todos fizessem parte e tivessem controle sobre esse poder. Esse sentimento leva as pessoas a direcionarem suas aspirações para o poder da nação como um todo, vendo-o como parte essencial de suas identidades e dos valores.

> O poder, quando perseguido como um objetivo em si mesmo pelo indivíduo, é considerado um mal a ser tolerado somente dentro de certos limites e em certas manifestações. O poder, quando dissimulado por ideologias e buscado em nome e para o bem da Nação, torna-se um bem para cuja consecução todos os cidadãos devem lutar (Morgenthau, 2003, p. 202-203).

Esse sentimento de orgulho nacional é reforçado pelos símbolos como bandeiras, hinos, brasões, especialmente ligados às Forças Armadas. Esses símbolos exercem o papel de fortalecimento dos laços entre os cidadãos e o Estado. Por outro lado, a insegurança e a sensação de falta de controle do Estado, especialmente entre aqueles com situação socioeconômica mais frágil, contribuem para que as pessoas se sintam frustradas quanto à própria vida. Essa frustração se intensifica ainda mais com a fragmentação social e a fragilidade dos laços comunitários. Ao se sentirem incapazes de controlar suas vidas individualmente, os indivíduos buscam significado e senso de pertencimento por meio da identificação com a força coletiva e com o prestígio associado à nação (Morgenthau, 2003).

Na definição da Escola Superior de Guerra (2009, p. 31), encontrada também Livro Branco de Defesa Nacional (Brasil, 2020c, p. 193)[29], o Poder Nacional pode ser compreendido como "a capacidade que tem o conjunto de homens e meios que constituem a Nação para alcançar e manter os Objetivos Nacionais em conformidade com a Vontade Nacional". Destacam-se nesse conceito, como elementos fundamentais, as pessoas que compõem a sociedade (Homem), a intenção coletiva da sociedade em relação aos assuntos nacionais (Vontade) e os recursos disponíveis para influenciar e alcançar objetivos (Meios). Os Objetivos Nacionais (ON) são as metas que o país busca alcançar para promover o bem-estar e o desenvolvimento de sua população. Eles são definidos com base nas necessidades, interesses e aspirações da sociedade em diferentes períodos de sua história e evolução cultural, visando atender aos desafios e oportunidades específicos que se apresentam ao país.

O conceito de Poder Nacional destaca o quão complexas e variadas são as capacidades de uma nação. Essas capacidades estão ligadas aos Objetivos Nacionais, que visam a promoção do desenvolvimento, a garantia da segurança e o bem-estar da população. Esse sistema é dinâmico e influenciado por muitos fatores, como as habilidades das pessoas envolvidas e os recursos disponíveis. Tais elementos afetam diretamente como o Poder Nacional se manifesta em diferentes contextos. Embora seja considerado como único e indivisível quando colocado em prática, sua natureza sistêmica permite que seja dividido para análise, facilitando o entendimento de suas características e importância (ESG, 2009).

O Estado, como instituição central designada pela Nação para representá-la, desempenha um papel fundamental na unificação, expressão e exercício do Poder Nacional. Essa responsabilidade é delegada, e permite não apenas a formulação e execução de processos político-jurídicos, mas também a coordenação da vontade coletiva e a aplicação consistente de uma parte substancial desse poder. Além disso, existe uma interdependência entre os aspectos internos e externos do poder estatal, ratificando a importância de um planejamento estratégico que leve em conta tanto as dinâmicas regionais quanto globais (ESG, 2009).

O Poder Nacional, em termos simples, é a capacidade de um Estado de alcançar seus objetivos, tanto dentro do seu próprio território quanto no cenário internacional. Isso envolve muito mais do que apenas o poder militar; inclui também as dimensões política, econômica, social, cultural e todas as outras áreas que ajudam a fortalecer a influência de um país. Esse poder se baseia em três pilares principais: o ser humano, a terra e as instituições. O ser humano é o núcleo dos valores e o motor do poder de uma nação; a terra é a base física que sustenta o

[29] Até ao momento de finalização dessa pesquisa, a nova versão do LBDN encontrava-se em processo de elaboração pelos órgãos competentes.

país; e as instituições organizam a vida dessa comunidade, em áreas como política, economia, defesa e tecnologia. Esses elementos do Poder Nacional se conectam e trabalham juntos para garantir o desenvolvimento e a segurança do Estado (ESG, 2024).

Como representação de um sistema social, o Poder Nacional reflete a estrutura da comunidade e manifesta seus fundamentos em cinco expressões, que são a política, econômica, psicossocial, militar e científico-tecnológica. Cada expressão reflete aspectos essenciais da força de uma nação, e pode ter efeitos que se estendem além de sua área específica, influenciando outras expressões. Ainda que não possam ser consideradas de maneira isolada, não funcionam de forma totalmente separada umas das outras, englobando elementos de várias naturezas: "em função de situações conjunturais, qualquer uma das Expressões pode ganhar relevância e projeção. No entanto, o caráter de unidade do Poder Nacional não se perde" (ESG, 2024, p.30).

A Expressão Política do Poder Nacional refere-se à maneira como a Nação se manifesta politicamente, através de instituições e grupos que interpretam os interesses e aspirações do povo e buscam estabelecer objetivos nacionais. Isso acontece por meio de interações entre essas entidades, que representam a vontade popular e transformam suas ações em normas e decisões. O Estado, como instituição soberana, pode impor coercitivamente ações que estejam alinhadas com a Vontade Nacional – que é a disposição coletiva da população de uma nação para alcançar seus objetivos e defender seus interesses –, exercendo assim a coerção social em benefício da sociedade. Em regimes democráticos, o Estado compartilha parte do poder com outras entidades para garantir um regime de liberdade equilibrado (ESG, 2024).

A Expressão Econômica do Poder Nacional envolve todas as atividades relacionadas à produção, distribuição e consumo de bens e serviços, tanto dentro quanto fora do país, de forma a alcançar e manter os Objetivos Nacionais. Isso implica a utilização consciente de seus recursos humanos e materiais a fim de alcançar o desenvolvimento e bem-estar social. Essa busca não é apenas materialista, as considerações éticas também são essenciais para garantir que o exercício do Poder Nacional esteja alinhado com os valores da sociedade (ESG, 2024).

A Expressão Militar do Poder Nacional consiste no uso ou na intenção do uso da força militar com a finalidade de prevenir, dissuadir ou neutralizar possíveis ameaças à segurança da nação. Ela abrange todos os aspectos relativos à defesa de um país, como orçamento militar, forças armadas, equipamentos, a estratégia de defesa, treinamento militar e a capacidade de projetar poder além das suas fronteiras. O poder militar de uma nação influencia não só a sua segurança interna, mas também afeta sua posição internacional, sua capacidade de dissuadir ameaças e sua influência geopolítica (ESG, 2024).

A Expressão Científica e Tecnológica do Poder Nacional abrange todos os recursos humanos, financeiros e materiais de uma nação destinados à geração, disseminação e aplicação dos conhecimentos científicos e tecnológicos, visando impulsionar seu desenvolvimento, competitividade e influência na estrutura global. Ela vai além da mera produção de conhecimento, se configurando como um instrumento estratégico fundamental para o desenvolvimento, competitividade e influência de um país no âmbito global. Através da mobilização de recursos humanos, financeiros e materiais, essa expressão impulsiona a geração, disseminação e aplicação de conhecimentos científicos e tecnológicos, resultando em um impacto profundo em diversas áreas da sociedade (ESG, 2024).

A Expressão Psicossocial do Poder Nacional abrange um amplo conjunto de elementos como pessoas, ideais, instituições, normas, estruturas, grupos, comunidades, recursos e organizações. Todos esses componentes são voltados para alcançar objetivos sociais importantes que satisfaçam as necessidades, interesses e aspirações da sociedade. Essa expressão se dedica principalmente à participação dos cidadãos na vida comunitária, refletindo o nível de satisfação dos indivíduos em suas atividades e interações sociais. Além disso, procura compreender os fenômenos humanos e sociológicos por meio da psicologia e ciências sociais, promovendo a plena realização dos cidadãos e de sua contribuição para o desenvolvimento da sociedade (ESG, 2024).

Essa expressão é formada pelos elementos “pessoa”, “ambiente” e “instituições sociais”. Esses fundamentos atuam de forma sinérgica, formando a base sólida da força do país. A “pessoa”, como ser biopsicossocial, constitui o núcleo dessa estrutura, e é constituída por seus valores, identidade e potencial aplicados no desenvolvimento social. O “ambiente”, tanto natural quanto social, diz respeito às condições necessárias para o bem-estar e a realização plena da pessoa. As “instituições sociais”, por sua vez, funcionam como a estrutura que sustenta e direciona o potencial individual e coletivo, garantindo a coesão social, a segurança pública e o progresso da nação (ESG, 2024).

As instituições sociais sustentam essa estrutura do Poder Nacional, mas também são influenciadas por mudanças que podem ocorrer no ambiente social e nas dinâmicas individuais. Compreender essa complexa relação é uma tarefa desafiadora, principalmente porque essas alterações podem gerar efeitos antes que sejam reconhecidas, conforme explica a instituição:

> O desafio que se põe ante os estudiosos do Poder Nacional é o de compreender as alterações que ocorrem nas Instituições Sociais com reflexos na estrutura desse Poder, porquanto, muitas vezes, elas produzem efeitos antes mesmo que se tenha percebido a sua ocorrência (ESG, 2024, p. 80).

4.4 VULNERABILIDADES DA EXPRESSÃO PSICOSSOCIAL À GUERRA COGNITIVA NAS REDES SOCIAIS

A ESG (2024) destaca que, como parte essencial das transformações sociais, a pessoa e o bem comum devem estar acima das estruturas e grupos sociais. Cada pessoa é um valor fundamental, com direito à liberdade e dignidade, e não deve ser manipulada, sofrer restrições injustas ou ser vítima de violência, seja por parte do Estado ou de outras instituições. Por isso, é essencial que os processos socioculturais incentivem o desenvolvimento de indivíduos livres, cooperativos e conscientes da importância de sua participação social. Quando esse equilíbrio se perde, toda a sociedade corre risco.

Os eventos de 8 de Janeiro de 2023 no Brasil tiveram consequências políticas e sociais significativas (Congresso Nacional, 2023) e foram motivados por esse senso de pertencimento a uma causa coletiva, de acordo com análise do psicanalista Leandro Faro (2023). Baseando-se na teoria sobre as massas de Gustave Le Bon, o autor procura desvendar a motivação desencadeadora dos atos de vandalismo e de tentativa de ruptura democrática, cuja data se tornou um marco na história da democracia brasileira. Estimulada por um sentimento de fervor coletivo baseado em um "medo estrutural" e convencimento religioso, uma multidão envolta em motivações psicológicas e ideológicas, desencadeou ações depredatórias contra as sedes do Palácio do Planalto, Congresso Nacional e Supremo Tribunal Federal – símbolos do poder do Estado brasileiro.

Os atos de 8 de Janeiro guardam semelhança com a invasão do Capitólio dos EUA, ocorrida dois anos antes, em 6 de janeiro de 2021. Ambos tiveram prédios públicos vandalizados em meio a contestações aos resultados eleitorais. Na ocasião, apoiadores do então presidente Donald Trump interromperam a sessão conjunta do Congresso estadunidense, que estava sendo realizada para confirmar a vitória eleitoral de Joe Biden na eleição presidencial de 2020. Manifestantes que participavam de um comício pró-Trump conseguiram transpor as barreiras de segurança do prédio e irromperam em atos violentos no Capitólio e em seus arredores, provocando a morte de cinco pessoas, e colocando o Congresso em isolamento por boa parte da tarde (Spaulding; Nair, 2021).

Essas ações podem ser parcialmente explicadas, de acordo com Le Bon (1998, *apud* Faro, 2023), pelo que ele chama de "multidão psicológica", que é quando a individualidade se dissolve e os indivíduos se agrupam, formando uma entidade coletiva. Nesse estado, os sentimentos, ideias e ações individuais se orientam em uma mesma direção, seguindo uma "lei da unidade mental das multidões". Faro acrescenta que o anonimato, possibilitado pelos

acampamentos dos militantes em frente aos quartéis em várias localidades do país, e pela interação dos integrantes desses grupos por meio das redes sociais, conferiu ainda mais força ao movimento. Somado ao impacto das imagens compartilhadas online de maneira ampla e da disseminação das *fake news*, esse anonimato permitiu que indivíduos se engajassem de forma intensa, expressando suas opiniões e apoiando a causa sem temer possíveis repercussões pessoais.

O *policy paper* produzido por Ruediger e Grassi (2023) para o projeto da FGV Comunicação Rio, realizado em colaboração com a Embaixada da Alemanha no Brasil, revela que, ao examinar os casos da rede social X e do Telegram, os autores conseguiram analisar as redes de interações associadas a esse episódio. Além disso, eles identificaram o progresso do debate temático, com foco particular em questões intervencionistas e securitárias. Os pesquisadores constataram que os invasores aproveitaram o evento para se promoverem nas redes sociais como influenciadores, inflamando o pedido de intervenção militar e convocando uma "revolução verde e amarelo", utilizando símbolos nacionais para reafirmar seu patriotismo. Também espalharam informações falsas com o intuito de motivar os envolvidos, como a suposta chegada de uma "fragata russa com arma hipersônica". Além disso, houve pedidos de *impeachment* simultâneo de autoridades e denúncias de supostos infiltrados nos atos depredatórios.

Giuliano da Empoli, em sua obra "Os Engenheiros do Caos" (2019), traz reflexões que apoiam a ideia de que a disseminação de notícias falsas e teorias conspiratórias não é um fenômeno aleatório. Para ele, esse processo faz parte de uma estratégia calculada com o objetivo de influenciar a opinião pública, gerar discórdia e até interferir em eleições. Ele defende que a propagação de desinformação vai além da simples liberdade de expressão ou de falhas nos algoritmos das redes sociais; trata-se de uma manipulação intencional. Essa estratégia utiliza, de forma deliberada, emoções como o medo e o ódio para dividir e polarizar a sociedade, alcançando assim seus objetivos.

> Se o algoritmo das redes sociais é programado para oferecer ao usuário qualquer conteúdo capaz de atraí-lo com maior frequência e por mais tempo à plataforma, o algoritmo dos engenheiros do caos os força a sustentar que não importa a posição, razoável ou absurda, realista ou intergaláctica, desde que ela intercepte as aspirações e os medos – principalmente os medos – dos eleitores (da Empoli, 2019, p. 20).

No turbulento panorama atual, a verdade sofreu uma fragmentação sem precedentes, conforme descrito por Kakutami (2018). A crença na verdade absoluta deu lugar a uma

realidade relativa, moldada pelas lentes individuais. Fatos, antes considerados pilares da comunicação e do conhecimento, passaram a ser percebidos como substituíveis, construídas socialmente e manipuláveis. Esse novo paradigma, alcunhado de "pós-verdade", mergulhou a sociedade em um mundo polarizado, onde premissas e posições arraigadas por décadas foram subvertidas e substituídas por seus opostos.

Sobre essa "era da pós-verdade", Haiden (2018, *apud* Althuis; Haiden, 2018) sustenta que o fenômeno surgiu em 2016, destacando como evidência a eleição do presidente Donald Trump e o sucesso da campanha do *Brexit*. Para Kakutami (2018), que examinou a erosão da verdade e o surgimento de falsidades durante a gestão de Trump (2017-2021), essa ascensão da subjetividade marcou um deslocamento significativo na forma como a verdade é percebida e manipulada, com o presidente estadunidense e seus aliados usando fatos inverídicos, desinformação e propaganda para moldar a opinião pública e fragilizar o poder da mídia, da ciência e de outras instituições. A opinião, antes vista como mero complemento da informação, ascendeu ao posto de protagonista, deslegitimando o conhecimento factual. As emoções, por sua vez, ganharam força, subjugando a racionalidade e a análise crítica. Essa inversão de valores deu origem a um ambiente fértil para a proliferação de desinformação, *fake news* e teorias conspiratórias, que se espalham rapidamente pelas redes sociais e por outros canais de comunicação (Kakutami, 2018; Mueller, 2016).

O impacto dessa fragmentação da verdade se estende a diversos setores da sociedade, desde a política e a justiça até a ciência e a educação. À medida que o tempo avança, observa-se um declínio na confiança depositada nas instituições tradicionais, abrindo espaço para uma atmosfera marcada pela desconfiança e pelo ceticismo. O debate público se torna cada vez mais polarizado e acalorado, dificultando o diálogo construtivo e a busca de soluções consensuais em "mundo no qual as *fake news* e as mentiras são divulgadas em escala industrial por 'fábricas' de *trolls* russos [...] e espalhadas pelo mundo todo na velocidade da luz por perfis em redes sociais" (Kakutami, 2018, p. 9-10).

Arjun Narayan, ex-líder do setor de Confiança e Segurança do Google e da controladora do TikTok, a ByteDance, expressou a dificuldade no combate à desinformação online, salientando que os disseminadores muitas vezes estão em posição de vantagem em relação às suas vítimas: "Os atores de abusos geralmente estão à frente do jogo; é (jogo de) gato e rato. Você está sempre jogando e tentando recuperar" (Field; Vanian, 2023, s.p., tradução nossa)[30]. A maioria dessa dinâmica concentra-se na subjetividade da narrativa.

---

[30] *"Abuse actors are usually ahead of the game; it's cat and mouse. You're always playing catch-up".*

A ideia de "regimes de verdade" de Foucault (2016) é bastante pertinente para entender esse cenário. Segundo ele, a verdade não é algo estático, mas sim o resultado de discursos que determinam o que deve ser considerado verdadeiro ou falso. Cada sociedade, nesse sentido, cria suas próprias regras e sistemas que definem o que será aceito como verdade. Essa perspectiva é útil na análise das *fake news*, uma vez que elas ganham legitimidade dentro de um contexto social e político específico, onde redes de poder influenciam e controlam o que é apresentado como verdade (Pinheiro, 2021).

A relevância dessa fragmentação conceitual sobre a verdade pode ser constatada pela oficialização do conceito de "pós-verdade" pelo Dicionário Oxford. Em 2016, a publicação, reconhecida mundialmente pelo registro e definição de novas palavras e expressões, escolheu o termo como a palavra do ano. A inclusão desse neologismo reflete uma era na qual fatos objetivos, dados e estatísticas têm menos importância na interpretação da verdade do que o sentimentalismo e as convicções pessoais. Os editores conceituam a "pós-verdade" como "circunstâncias em que os fatos objetivos são menos influentes em formar a opinião pública do que os apelos à emoção e à crença pessoal", destacando a crescente importância da percepção subjetiva sobre a objetividade factual em questões políticas, sociais e culturais na atualidade (Oxford Learner's Dictionaries, 2016, s.p., tradução nossa)[31].

O analista e estrategista Alexander Dugin, representante da visão ultranacionalista e de defensores da extrema direita russa (Mendonça, 2021), tem uma visão peculiar sobre a verdade que corrobora com o conceito da pós-verdade. Em uma entrevista concedida à *BBC Newsnight* em 2016, Dugin afirma que a verdade é uma questão de crença e que a existência objetiva dos fatos é questionável. Em sua visão de mundo, "ninguém tem o monopólio da verdade, ela é relativa" (BBC, 2016, 10'16", tradução nossa)[32]. Para ele, o que realmente importa não é a veracidade, mas sim a narrativa e o impacto que ela causa. Suas ideias encontram ressonância em grupos e movimentos políticos extremistas em várias partes do mundo.

Essa propagação de crenças, aliada a sentimentos conspiratórios e informações distorcidas, foi um dos fatores que levaram à mobilização articulada de pessoas contrárias ao resultado das eleições, segundo consta no relatório da CPI de 8 de Janeiro, divulgado pelo Congresso Nacional (2023). O documento afirma que os envolvidos nas ações estavam dispostos a enfrentar as forças de segurança para tentar "tomar o poder". De acordo com a investigação parlamentar, houve uma conexão direta entre a disseminação de desinformação e a motivação por trás dos atos de vandalismo e violência ocorridos na referida data:

---

[31] *"relating to circumstances in which people respond more to feelings and beliefs than to facts".*
[32] *"There's nobody has monopoly on the thruth. The truth is relative".*

> O 8 de Janeiro não foi um movimento espontâneo ou desorganizado: foi uma mobilização idealizada, planejada e preparada com antecedência. Os executores foram insuflados e arregimentados por instigadores, que definiram, de forma coordenada, datas, percurso e estratégias de enfrentamento e ocupação dos espaços. Caravanas foram organizadas de forma estruturada e articulada (Congresso Nacional, 2023, p.13).

Esse fenômeno revela uma progressão complexa, na qual a combinação entre a visibilidade midiática e o anonimato virtual impulsionou a mobilização e a identificação dentro do grupo, com o propósito de desestabilizar o Poder Nacional. As ações visavam a amplificação das narrativas extremistas para que encontrassem respaldo e, desta forma, viabilizassem a instalação de um estado de sítio: "O objetivo era um só: invadir ou deixar invadir as sedes dos Poderes, desestabilizar o Governo, incendiar o País, provocar o caos e a desorganização política — e até mesmo, se necessário, uma guerra civil" (Congresso Nacional, 2023, p.14).

Mendonça (2021) explica que a interconexão global das redes sociais possibilitada pela internet, juntamente com a afinidade às ideias de defensores da extrema direita, criou um ambiente favorável para que movimentos e agentes, antes considerados periféricos, influenciassem "audiências fiéis":

> A conectividade em massa e simultânea produzida pelas redes sociais e a internet, marca registrada da globalização, além de um alinhamento intelectual de pensadores da direita extrema ajudou a criar um cenário fértil para movimentos e atores antes obscuros ou não tão presentes no "mainstream", que encontraram um público fiel e uma influência em parte da extrema-direita global (Mendonça, 2021, p. 1).

Essa dinâmica encontra relativo respaldo na teoria do choque das civilizações, apresentada por Huntington (1996). Segundo esse fundamento, as principais fontes de conflito no mundo pós-Guerra Fria (1945-1991) não seriam mais predominantemente ideológicas ou econômicas, e sim culturais e religiosas, especialmente no que diz respeito a valores, crenças e identidades, que afetam o poder constituído de uma nação.

Na ótica de Huntington, a cultura e a religião desempenham um papel central na percepção em como as pessoas entendem quem são e a quem devem lealdade. Quando uma nação tem coesão cultural e um forte senso de pertencimento, isso fortalece a capacidade do Estado de exercer poder e influência no mundo. Mas, quando essas identidades nacionais e locais começam a enfraquecer, o fundamentalismo religioso pode emergir como uma maneira de recuperar essa sensação de identidade perdida. Huntington ainda aponta que os governos

acabam se aproximando da religião, já que ela pode abrir caminho para a criação de alianças políticas úteis.

Embora a teoria de Huntington se concentre nas relações internacionais e no potencial de conflito entre civilizações, é possível aplicá-la no âmbito doméstico para entender a fragmentação política, inquietação social e até violência, decorrentes de divisões étnicas, religiosas ou linguísticas dentro de um Estado. Nos meses que antecederam os atos de 8 de Janeiro de 2023, os militantes organizados na frente dos quartéis mencionavam Deus e família como elementos motivadores na defesa de uma intervenção militar (Toledo, 2022). Em casos extremos, divisões culturais profundas podem alimentar movimentos separatistas, onde grupos buscam se desvincular do Estado e estabelecer sua própria organização político-estatal independente (Huntington, 1996).

Ao destacar o papel da religião na formação da dinâmica política e na influência sobre o poder estatal, Huntington (1996) sugere, ainda, que o enfraquecimento das identidades nacionais ou locais pode levar ao surgimento do extremismo religioso como forma de afirmar a identidade cultural. Essa situação é capaz de se manifestar em movimentos fundamentalistas que desafiam a autoridade do Estado e promovem sua própria interpretação rígida da doutrina religiosa e social. O componente ideológico, ao encontrar neste caso respaldo em motivações políticas, se torna um ambiente fértil para a disseminação das notícias falsas.

Segundo Henry (2019), as *fake news* estão profundamente enraizadas em ideologias políticas. Não é somente a tecnologia digital que permite que a disseminação de falsas informações se alastrem, mas também um crescente acúmulo de ressentimentos e desconfiança da população em relação às grandes instituições. Esse mal-estar, que cresce com o tempo, faz com que os indivíduos fiquem mais dispostos a acreditar naquilo que reforça as suas frustrações e preconceitos.

A situação é dinamizada com a crescente polarização política, que não só divide a sociedade, mas forma também um ambiente propício para as lideranças de extrema direita ou de extrema esquerda se fortalecerem. As *fake news* se destacam ainda mais na desunião e disputa, porque são recebidas por um público mais disponível e ávido a crer em narrativas que confirmem suas convicções pessoais, ainda que não sejam verdadeiras (Henry, 2019).

O presente estudo tem revelado que os impactos da guerra cognitiva nas redes sociais são visíveis na manifestação psicossocial do Poder Nacional. Essa influência é particularmente marcante e significativa nessa expressão, afetando diversos aspectos e dinâmicas da sociedade, da política e das relações internacionais.

A guerra cognitiva é um fenômeno complexo que transcende as fronteiras tradicionais da guerra, envolvendo estratégias de manipulação de informações, influência psicológica e guerra de narrativas. Em um contexto global cada vez mais conectado e digitalizado, a disseminação rápida e abrangente de informações e narrativas pode ter um impacto profundo na percepção pública, na tomada de decisões políticas e até mesmo na estabilidade de regiões inteiras (Cluzel, 2020).

Além disso, a guerra cognitiva muitas vezes opera de maneira sutil e indireta no ambiente virtual, utilizando técnicas de propaganda, desinformação e manipulação emocional para moldar atitudes, crenças e comportamentos das pessoas. Isso pode resultar em divisões sociais, polarização política e até mesmo no enfraquecimento das instituições democráticas, minando assim a coesão e a governança de um país (Cluzel, 2020).

Considerando esses aspectos, fica evidente a importância de defender e fortalecer a Expressão Psicossocial do Poder Nacional como parte essencial da soberania nacional. A capacidade de proteger a integridade da informação, promover uma comunicação transparente e ética, e cultivar uma cultura de pensamento crítico e resistência à manipulação é fundamental para preservar a independência e a estabilidade de uma nação em meio aos desafios da guerra cognitiva.

4.5 A DEFESA DA EXPRESSÃO PSICOSSOCIAL NO CONTEXTO DA GUERRA COGNITIVA DIGITAL

O raciocínio de Nye Jr. (2004) de que o s*oft power* e a capacidade de influenciar a percepção pública são relevantes para o sucesso da política externa e para a defesa da soberania nacional constitui um bom fundamento para entender a importância da proteção da Expressão Psicossocial para fins de proteção da soberania nacional. Promover uma Expressão Psicossocial forte, por parte de um Estado, é uma forma de aumentar seu *soft power* e também contribui para influenciar, de maneira positiva, outros atores internacionais. Esta estratégia, pode incluir a defesa de sua cultura, valores democráticos, respeito aos direitos humanos, bem como seu compromisso com a paz e sua disposição para uma estrutura de cooperação global.

O conceito fornecido pela ESG em 2024, que se alinha à perspectiva de Joseph Nye Jr. sobre *soft power,* destaca a ideia de que a Expressão Psicossocial de um país vai além da simples capacidade de comunicar mensagens internacionalmente. Não se trata apenas de disseminar informações ou promover uma imagem positiva, mas de influenciar profundamente como

outros países e populações percebem, interpretam e reagem às ações, valores e identidade de do Estado.

O *soft power* não é exclusivo das instituições e governos, ele pode ser desenvolvido e aplicado também por atores não estatais, como a sociedade civil, o terceiro setor e outras organizações. Esses agentes podem criar e implementar estratégias de poder sutis para influenciar as políticas e estratégias de relações exteriores de um Estado, tanto de maneira positiva quanto negativa (Nye Jr., 2004). Em um mundo cada vez mais interconectado e influenciado pela comunicação e pela percepção pública, essa estratégia se torna ainda mais dinâmica e persuasiva, com a disseminação de desinformação e narrativas manipuladoras nas redes sociais, afetando a Expressão Psicossocial. Conforme alerta Kakutani (2018, p. 52, tradução nossa)[33], isso se reflete na "crescente desorientação que as pessoas vêm sentindo por conta da desconexão entre o que sabem ser verdade e o que os políticos dizem, entre o senso comum e o funcionamento do mundo".

A guerra cognitiva nas redes sociais pode afetar os fundamentos da Expressão Psicossocial do Poder Nacional, mudando a maneira como os indivíduos percebem e interpretam os valores e princípios que formam a sociedade. A disseminação de informações distorcidas ou manipuladas tem potencial para desestabilizar o tecido social e os fundamentos nacionais, levando a uma fragmentação da identidade cultural e social (Cluzel, 2020). Quando essas informações falsas ou tendenciosas são amplamente difundidas e recebem atenção nas plataformas digitais, elas podem fazer com que as pessoas enxerguem o mundo ao seu redor de maneira distorcida, influenciando suas opiniões sobre diversos assuntos (Kakutami, 2018).

A disseminação de conteúdos tendenciosos e manipulados por meio das redes sociais pode distorcer a percepção que as pessoas têm sobre a realidade ao seu redor. A propagação de discursos de ódio e de desinformação interfere na harmonia e estabilidade social ao se constituir em uma fonte de tensões e de conflitos. Por outro lado, a formação de bolhas de informação dificulta que o indivíduo tenha contato com diferentes pontos de vista, reforçando suas crenças e comprometendo o entendimento do contexto social e político (Althuis; Haiden, 2018).

Diante dessas constatações, entende-se que a disseminação de informações distorcidas, *fake news* e discursos de ódio não apenas altera a percepção individual das pessoas, mas também contribui para a fragmentação da coesão social, reduzindo a confiança nas instituições e comprometendo a estabilidade democrática de um país, afetando de forma significativa a Expressão Psicossocial do Poder Nacional. A guerra cognitiva nas redes sociais pode, desta

[33] *"the burgeoning disorientation people have been feeling over the disjuncture between what they know to be true and what they are told by politicians, between common sense and the workings of the world".*

forma, distorcer a percepção da democracia como um objetivo fundamental, erodindo o respeito à dignidade da pessoa, à liberdade e à igualdade de oportunidades (Cluzel, 2020).

Em sua pesquisa para o *Internet Observatory* em Stanford, John (2021) descreveu o efeito das campanhas de influência externa em plataformas de redes sociais, e apontou uma tendência preocupante que está acontecendo entre os jovens. Ele afirma que essa parcela da população, que em breve estará em cargos com poder de tomada de decisões, está cada vez mais moldada pelas informações que circulam no ciberespaço. Segundo ele, uma pesquisa da *Common Sense Media,* mostra que, em vez de buscar fontes de notícias tradicionais, 60% dos jovens se informam com influenciadores digitais. Eles também estão mais dispostos a acreditar em desinformação e má informação e depois repassá-las adiante, especialmente se houver identificação com a pessoa que criou a informação originalmente.

Essa constatação acende um alerta sobre o potencial da manipulação das narrativas no ambiente digital. No contexto multipolarizado da era da informação, onde diferentes Estados e organizações competem pelo domínio da narrativa e pela influência global, o controle da opinião pública para fins diversos por meio das redes sociais torna-se uma estratégia central. Desta forma, a defesa da Expressão Psicossocial contra a guerra cognitiva emerge como um compromisso inadiável para fortalecer a coesão social e assegurar a autonomia do país. É um esforço contínuo e emergente, que exige a participação de todos os setores da sociedade. Essa perspectiva consolida os argumentos apresentados no capítulo, destacando a relevância estratégica dessa dimensão do Poder Nacional na salvaguarda dos interesses nacionais.

5 ABORDAGENS METODOLÓGICAS

Neste capítulo, são apresentadas as abordagens metodológicas utilizadas na construção deste Trabalho de Conclusão de Doutorado (TCD), que tem por objetivo fornecer subsídios para a formulação de políticas públicas pelo Ministério da Defesa contra as ameaças à Expressão Psicossocial do Poder Nacional decorrentes da guerra cognitiva nas redes sociais. O detalhamento dos métodos e técnicas empregados, acompanhados das justificativas que sustentam cada escolha, evidenciam a consistência do estudo.

A pesquisa foi estruturada em cinco fases principais, que são: pesquisa exploratória; pesquisa bibliográfica; revisão da literatura; aplicação dos métodos *ex-post facto* e comparativo; e *survey*. As seções a seguir apresentam os delineamentos metodológicos adotados, incluindo os procedimentos, os instrumentos e técnicas de coleta de dados, os critérios de seleção dos participantes, os processos de análise e interpretação dos resultados, bem como as considerações éticas que nortearam a condução do estudo.

5.1 MÉTODO DE PESQUISA

5.1.1 Natureza e justificativa do método

A abordagem metodológica dessa pesquisa é de natureza qualitativa, pois se concentra na dinâmica das relações sociais, explorando aspectos da realidade social que não podem ser mensurados. Creswell (2014) assinala que estudos qualitativos permitem um entendimento mais abrangente dos fenômenos, considerando os diversos fatores sociais, culturais e comportamentais envolvidos. Deste modo, o método qualitativo se apresenta como o mais indicado para o estudo da guerra cognitiva nas redes sociais, pois permite a análise das narrativas dos ambientes virtuais, propicia um entendimento da manipulação e disseminação das informações e contribui para a identificação das diferentes táticas de desinformação.

5.1.2 Procedimentos metodológicos adotados

5.1.2.1 Pesquisa exploratória

Com a metodologia definida, realizou-se uma revisão exploratória da literatura para contextualizar e fundamentar a importância do estudo. Conforme explica Gil (2007), esse

método permite identificar as principais teorias, conceitos, modelos e abordagens relacionadas ao tema da pesquisa que, neste estudo, diz respeito à guerra cognitiva nas redes sociais e as possíveis ameaças à Expressão Psicossocial do Poder Nacional brasileiro. Com base nas informações obtidas, delineou-se a problemática do estudo, levando em conta o "estado da arte", as lacunas existentes e a relevância do tema.

Esse levantamento preliminar identificou um aumento significativo no cenário global de estratégias de guerra cognitiva empregada por Estados e atores não estatais nas redes sociais. Também foi possível verificar a existência de uma intensificação dessas estratégias no contexto brasileiro, utilizadas por agentes internos. Tais ações tinham como propósito moldar os pensamentos e comportamentos dos indivíduos ao influenciar seus processos cognitivos por meio do controle da narrativa e da informação.

Com a problemática identificada, a pergunta de pesquisa foi formulada para orientar o processo investigativo, a fim de obter respostas objetivas e aprofundadas sobre o fenômeno em estudo. Posteriormente, procedeu-se à definição dos objetivos, que serviram para orientar a pesquisa, definir métodos e avaliar resultados, garantindo a execução do trabalho de forma eficaz e relevante (Gerhardt; Silveira, 2009).

5.1.2.2 Pesquisa bibliográfica

Em aprofundamento à fase exploratória, realizou-se um extenso levantamento bibliográfico com o intuito de examinar a literatura correspondente ao objeto de estudo, tanto as obras clássicas quanto as contemporâneas, a fim de fornecer a base teórica para a pesquisa. Esta fase permitiu contextualizar o tema de estudo, propiciando uma compreensão mais definida que já fora discutido. Como abordado por Petticrew e Roberts (2006), a pesquisa bibliográfica é uma etapa preliminar e necessária à revisão de literatura, tendo como foco a reunião e organização da informação relevante para um determinado tema.

5.1.2.3 Revisão da literatura

Posteriormente, foi conduzida uma revisão da literatura para fundamentar teoricamente o estudo, reforçar a relevância do problema, consolidar a compreensão sobre o objeto estudado, e identificar de forma mais precisa as lacunas existentes. Essa etapa envolveu uma abordagem mais rigorosa e estruturada, com critérios de inclusão e exclusão bem definidos, para garantir

que todas as fontes relevantes fossem consideradas de maneira imparcial e dentro da abrangência do escopo da pesquisa (Petticrew; Roberts, 2006).

A revisão da literatura desempenha um papel de grande importância em qualquer pesquisa acadêmica, visto que proporciona a fundamentação teórica e metodológica para a elaboração de novos estudos (Triviños,1987). O método foi utilizado para contextualizar a pesquisa no que se refere a teorias e conceitos significativos para este estudo.

Adicionalmente, a revisão da literatura ampliou a compreensão de estratégias e conceitos relevantes, como curadoria algorítmica; inteligência artificial e hiperinteligência; operações de influência e de retórica, *digital astroturfing*, infodemia, desinformação e *fake news*, além de seus efeitos como polarização e divisão social; vigilância e manipulação de dados pessoais; desinformação, manipulação informacional, psicologia das massas e segurança informacional, todos essenciais para uma compreensão completa do fenômeno.

Ao revisar a literatura, foi possível perceber que faltam estudos sobre a eficácia das estratégias para combater as ameaças da guerra cognitiva nas redes sociais, especialmente no contexto do Brasil. O método também possibilitou identificar que o país não possui políticas públicas específicas para enfrentar essas ameaças, que muitas vezes vêm de atores estrangeiros. Essa análise, no entanto, ajudou a construir uma base teórica sólida para a pesquisa, além de viabilizar o suporte conceitual indispensável para o avanço do estudo em questão.

5.1.2.4 Métodos ex-post facto e comparativo

A partir das etapas anteriores estabelecidas, optou-se por aplicar o método *ex-post facto* para analisar as campanhas de guerra cognitiva da Rússia, China e Cambridge Analytica nesse ambiente. Esses casos servem como exemplos significativos para o entendimento das dinâmicas e tendências emergentes nesse domínio, devido à relevância desses atores como foco de estudos acadêmicos e de defesa globais.

O levantamento *ex-post facto* se justifica pela necessidade de reconstruir e analisar os eventos e ações relacionados à guerra cognitiva. Também permite compreender o desenvolvimento e evolução ao longo do tempo dos casos estudados, contribuindo para um entendimento mais aprofundado desse fenômeno. O método *ex-post facto* é apresentado por McMillan e Schumacher (2006) como uma abordagem relevante para a pesquisa descritiva, permitindo a investigação e análise de fenômenos e acontecimentos do passado e sua influência no presente. Os dados retrospectivos são analisados para identificar e comparar dois ou mais grupos que diferem em uma variável-chave. A finalidade é verificar as diferenças em suas

abordagens e identificar padrões e tendências que possam ajudar a compreender as estratégias escolhidas. Associado a esse método, foi aplicada a análise comparativa, com base nas abordagens de Przeworski e Teune (1970), Anckar (2008) e Lijphart (1971).

5.1.2.5 Survey

Por fim, foi aplicada uma *survey* por meio de formulário online, com especialistas de diversas áreas relacionadas ao tema da pesquisa. Essa etapa buscou conferir a aplicabilidade e relevância prática, no contexto brasileiro, dos conceitos e modelos abordados, complementando a investigação anteriormente conduzida. Essa abordagem metodológica integrada permitiu uma compreensão mais ampla e multifacetada do fenômeno em questão.

Com a finalidade de identificar quais abordagens estão sendo empregadas contra essas ameaças, também foi realizada uma revisão bibliográfica e de documentos que abordam as iniciativas de diversos Estados, grupos internacionais e agências especializadas, contra a desinformação nas redes sociais, o que contribuiu significativamente para o alcance dos objetivos da pesquisa. Ao examinar essas estratégias, foi possível obter uma visão abrangente das práticas mais eficazes em diferentes contextos. Essa análise permitiu identificar tendências, lacunas e lições aprendidas, fornecendo um importante fundamento para o desenvolvimento de políticas voltadas para o combate ao fenômeno da guerra cognitiva online. Além disso, as experiências internacionais agregaram conhecimentos valiosos para a formulação de iniciativas adaptadas à realidade nacional, contribuindo para fortalecer as instituições e a sociedade contra a disseminação a manipulação cognitiva nas redes sociais.

A pesquisa *survey* foi empregada em conjunto com a análise comparativa e a revisão de literatura para realizar uma triangulação metodológica. Neste método de pesquisa obtêm-se dados ou informações sobre as características ou opiniões de determinado grupo de pessoas, utilizando um questionário como instrumento (Fonseca, 2002). Os resultados obtidos através da *survey* foram confrontados e validados com os achados da análise comparativa e da revisão bibliográfica. Essa comparação possibilitou a identificação de convergências e divergências nos dados, enriquecendo a análise e proporcionando uma visão mais robusta e detalhada do objeto de pesquisa.

A *survey* foi realizada com 25 especialistas das áreas de segurança e defesa, tecnologia da informação, ciências políticas, comunicação e psicologia. Essa diversidade de conhecimentos ajudou a aprofundar a compreensão sobre o tema. Os especialistas foram escolhidos com base nas áreas identificadas como relevantes para a guerra cognitiva durante a

revisão de literatura. Ao incluir profissionais de diferentes disciplinas, foi possível enriquecer a análise, considerando várias perspectivas e expertises. Essas descobertas valiosas foram fundamentais para entender de forma abrangente os aspectos técnicos, políticos, sociais e psicológicos envolvidos na guerra cognitiva nas redes sociais.

5.2 LIMITAÇÕES DO ESTUDO

Toda pesquisa, enfrenta limitações independentemente do método utilizado. Segundo Lijphart (1971), a análise comparativa também apresenta restrições, embora forneça benefícios importantes. Uma delas é o controle de variáveis. Nesse método, o pesquisador tem o desafio de isolar todas as variáveis que podem afetar o resultado. Isso dificulta o estabelecimento das relações causais entre elas. Por conta disso, reduz a capacidade de generalizar os resultados em outros contextos ou afirmar a causalidade de uma variável específica. Para minimizar esses impactos, Lijphart indica como cuidados adicionais a seleção cuidadosa de casos e a triangulação com outras abordagens metodológicas.

Outro fator limitador diz respeito à *survey*, que não garante relatos completamente imparciais e neutros. Isto porque, como ressaltado por Gioia *et al* (2013), os respondentes são inevitavelmente influenciados pelas memórias, opiniões e vieses cognitivos, o que impossibilita considerá-los completamente isentos.

Por outro lado, o tema da pesquisa é algo complexo, que enfrenta várias limitações, como a própria natureza dinâmica e imprevisível da guerra cognitiva. A intensificação desse tipo de conflito nas redes sociais em nível global representa um desafio significativo para a pesquisa acadêmica nesse campo. As estratégias e narrativas utilizadas mudam rapidamente, dificultando a análise e a interpretação consistentes.

Outro fator agravante é a sua constante evolução na forma e métodos utilizados pelos atores para influenciar narrativas e manipular a percepção pública por meio das campanhas de desinformação, propaganda e outras técnicas sofisticadas. Fenômenos emergentes, como a disseminação “viral” de conteúdo falso ou o surgimento repentino de novas plataformas de interação online, evoluem de maneira tão dinâmica que frequentemente ultrapassam o ritmo dos procedimentos tradicionais de investigação acadêmica.

A insuficiência de estudos sobre a dinâmica da guerra cognitiva no Brasil apresenta um desafio significativo para os formuladores de políticas públicas. Essa escassez é um complicador a mais, pois impacta a identificação de padrões e tendências nas estratégias

empregadas. Isso, por sua vez, prejudica a construção de uma base teórica sólida e abrangente, afetado a elaboração de medidas necessárias para que o país se proteja das ameaças emergentes.

Concomitantemente, a variedade e a complexidade das iniciativas que almejam combater a desinformação e a manipulação cognitiva também representam um obstáculo significativo. Desde ações governamentais até projetos da sociedade civil, uma quantidade praticamente inesgotável de abordagens e ferramentas são desenvolvidas, tornando difícil estabelecer parâmetros e métricas de avaliação consistentes.

De forma complementar, a atribuição de causas específicas sobre os efeitos observados da guerra cognitiva se apresenta como uma tarefa complexa por causa da influência das diversas variáveis. Essa complexidade dificulta determinar de maneira específica como as operações relacionadas à guerra cognitiva impactam a Expressão Psicossocial do Poder Nacional. Também prejudicam a mensuração de seus efeitos, uma vez que os resultados tendem a ser sutis.

Para finalizar, a falta de transparência no funcionamento dos algoritmos e a restrição na obtenção de dados sobre as plataformas de redes sociais impossibilitam a realização de uma análise abrangente, e às vezes até adequada, do fenômeno da guerra cognitiva nesses ambientes. Isso traz outros desafios relacionados à ética, incluindo privacidade de informações, controle de informações e liberdade de expressão. Portanto, para lidar com tais limitações, é importante adotar abordagens que incentivem a interação de diferentes campos do estudo a fim de formular planos e métodos que neutralizem tais ameaças.

5.3 SURVEY: RESULTADOS E DESCOBERTAS

A análise de dados é uma etapa fundamental em qualquer pesquisa científica. Seu propósito é organizar e interpretar os dados coletados e, assim, fornecer respostas para o problema proposto. Com essa perspectiva, a realização da *survey* seguiu as etapas comumente identificadas na literatura, conforme apontado por Gil (1999). Primeiramente, os dados foram agrupados e categorizados observando as características comuns. Em seguida, a codificação e a tabulação permitiram transformar esses dados em um formato adequado para análise. Por fim, as informações tabuladas foram analisadas estatisticamente, o que permitiu uma interpretação objetiva e fundamentada das informações coletadas durante a pesquisa.

O questionário consistiu em cinco questões fechadas e uma aberta. A quinta questão, além de ser de múltipla escolha, permitiu que o respondente incluísse uma resposta escrita. Com isso, pretendeu-se obter informações não previstas nos enunciados a fim de enriquecer a análise dos dados com significados subjacentes aos resultados numéricos (Gerhardt; Silveira, 2009). Essa combinação de métodos quantitativos e qualitativos possibilitou uma análise abrangente e consistente do conteúdo obtido por meio da *survey*, agregando informações relevantes às questões relacionadas à guerra cognitiva, segurança nacional e influência das redes sociais, ao mesmo tempo em que forneceu dados estatísticos para embasar as conclusões e recomendações apresentadas no estudo.

Além das tabelas com a tabulação da pesquisa on-line, foram incluídos gráficos a fim de fornecer uma percepção visual mais refinada dos resultados. Esses gráficos foram projetados para destacar as descobertas mais significativas relativas a cada pergunta, facilitando a interpretação dos dados. Essa abordagem visual permite uma análise mais intuitiva e abrangente, possibilitando a rápida identificação de padrões e *insights* relevantes. A combinação de tabelas e gráficos oferece uma visão mais completa e acessível dos resultados da pesquisa.

6.1 Primeira pergunta

A grande maioria dos especialistas (70%; 16) considera que a abordagem do Domínio Humano é extremamente relevante para o desenvolvimento de estratégias de defesa do Estado brasileiro. O alto percentual de concordância entre os respondentes revela que as operações militares e de segurança devem incluir as questões relacionadas à cognição, à informação e outras dimensões humanas.

O resultado demonstra que entender e incorporar o domínio humano nas estratégias de defesa é fundamental para a estabilidade e integridade do país no contexto internacional. A percepção compartilhada pelos especialistas reforça que é necessária uma abordagem holística que considere esse elemento na formulação e implementação de políticas de segurança nacional, tanto em relação aos aspectos técnicos e operacionais, como aos relativos às pessoas.

Ainda referente a essa questão do Domínio Humano, um número significativo de especialistas (26%; 6) atribui a abordagem como muito relevante, embora em uma escala ligeiramente menor do que aqueles que a consideram extremamente relevante. Apenas um participante (4%) classificou a abordagem como relevante, mas não como a mais importante, expressando uma visão mais moderada.

Tabela 2 – Análise quantitativa das respostas da 1ª pergunta

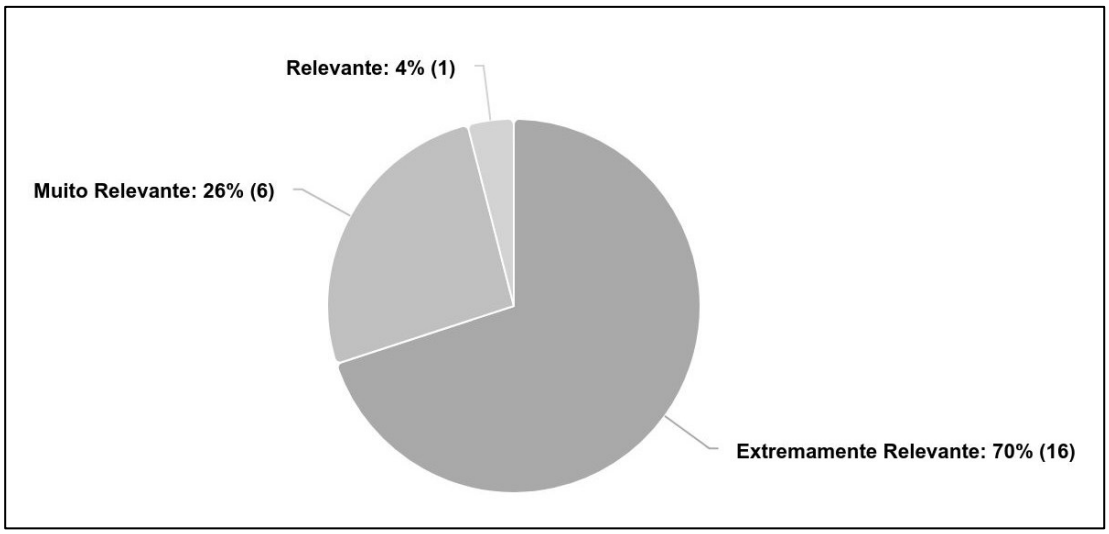
ENUNCIADO: Segundo a OTAN (Cole; Guyader, 2021), o Domínio Humano é o centro de todos os outros domínios, e deve ser considerado a pedra angular que sustenta a estabilidade e a integridade do cenário internacional. Este conceito reconhece a importância das questões relacionadas à cognição, à informação e a outras dimensões humanas relacionadas, como parte integrante das operações militares e de segurança. Diante dessa perspectiva, o quanto você considera relevante essa abordagem para o desenvolvimento de estratégias de defesa do Estado brasileiro?

COLE, A.; LE GUYADER, H. *NATO sixth's domain of operations*. In Silico: The Speech That Never Was. [S.l.]: [s.n.], p. 29, 2021

ALTERNATIVAS	Frequência	Relevância
Extremamente relevante (Essa abordagem não pode faltar nas estratégias de Defesa)	16	70%
Muito relevante (Essa abordagem é relevante e deve ser considerada)	6	26%
Relevante (Essa abordagem é relevante, mas não é a mais importante)	1	4%
Pouco relevante (Essa abordagem tem pequena relevância, mas não é essencial)	0	0%
Irrelevante (Essa abordagem não precisa ser considerada)	0	0%

Fonte: Elaborado pela autora.

Gráfico 1 – Representação visual dos resultados da 1ª pergunta



Fonte: Elaborado pela autora.

Tabela 3 – Análise das respostas da 1ª pergunta, por perfil profissional

PERFIL PROFISSIONAL	Frequência	Relevância
Oficial Superior das Forças Armadas	10	6 (27%) - Extremamente Relevante 3 (13%) - Muito Relevante 1 (4%) - Relevante
Jornalista e Professor	2	2 (9%) - Extremamente Relevante
Especialista em Tecnologia da Informação	2	2 (9%) - Extremamente Relevante
Especialista em Segurança Cibernética	1	1 (4%) - Extremamente Relevante
Pós-graduando em Defesa Cibernética	1	1 (4%) - Extremamente Relevante
Doutora em Ciências Navais	1	1 (4%) - Extremamente Relevante
Mestre em Ciências Políticas	1	1 (4%) - Extremamente Relevante
Mestre em Defesa Nacional	1	1 (4%) - Extremamente Relevante
Especialista em psicologia militar	1	1 (4%) - Extremamente Relevante
Professor em Ciências da Computação	1	1 (4%) – Extremamente Relevante
Doutor (a) em Ciências Políticas	2	2 (9%) - Muito Relevante

Fonte: Elaborado pela autora.

6.2 Segunda pergunta

Em relação à percepção sobre a pertinência das redes sociais para o êxito da guerra cognitiva, 60,9% dos respondentes (14) apontam que essas plataformas desempenham um papel extremamente importante na disseminação da desinformação e suas implicações estratégicas relacionadas à segurança nacional e política internacional, entre outras.

Embora em uma escala ligeiramente menor do que aqueles que as consideraram extremamente importante, um número significativo de especialistas (34,8%; 8) reconhecem o papel significativo dessas ferramentas como componentes valiosos da estratégia de comunicação e influência.

Uma pequena porcentagem dos especialistas (4,3%; 3) expressou uma visão mais moderada em relação à importância das redes sociais na guerra cognitiva. Eles reconhecem que essas ferramentas têm alguma influência na disseminação de informações estratégicas, porém consideram-na como moderada em relação ao contexto mais amplo da guerra cognitiva.

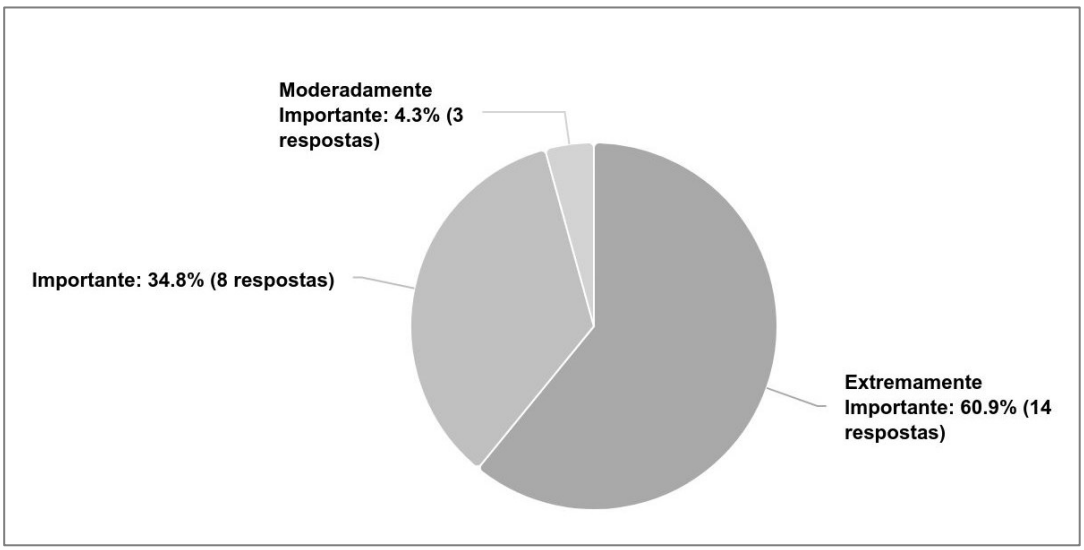
Tabela 4 – Análise quantitativa das respostas da 2ª pergunta, por importância

ENUNCIADO: Dentro do contexto das estratégias contemporâneas para alcançar o Domínio Humano, os autores destacam a guerra cognitiva, que utiliza a desinformação e afirmativas falsas como armas para influenciar a opinião pública e moldar a percepção da realidade. Em um mundo hiperconectado, onde a troca de informações é cada vez mais intensa por meio das redes sociais, qual é a magnitude da importância dessas plataformas na disseminação de informação estratégica em âmbito global?		
ALTERNATIVAS	**Frequência**	**Importância**
Extremamente Importante: As redes sociais desempenham um papel fundamental na disseminação de informações estratégicas globalmente, sendo ferramentas indispensáveis na guerra cognitiva.	14	60,9%
Importante: As plataformas de redes sociais têm um papel significativo na disseminação de informações estratégicas, desempenhando um papel relevante no contexto da guerra cognitiva.	8	34,8%’
Moderadamente Importante: Embora as redes sociais tenham alguma influência na disseminação de informações estratégicas, é considerada moderada em relação à guerra cognitiva.	3	4,3%
Pouco Importante: As redes sociais desempenham um papel restrito na disseminação de informações estratégicas em escala global, apresentando impacto limitado na guerra cognitiva.	0	0%

ALTERNATIVAS	Frequência	Importância
Irrelevante: O papel das redes sociais na disseminação de informações estratégicas no âmbito global é insignificante e não apresenta riscos.	0	0%

Fonte: Elaborado pela autora

Gráfico 2 – Representação visual dos resultados da 2ª pergunta



Fonte: Elaborado pela autora

Tabela 5 – Análise das respostas da 2ª pergunta, por perfil profissional

PERFIL PROFISSIONAL	Frequência	Relevância
Oficial Superior das Forças Armadas	10	4 (17,4%) – Extremamente Importante 5 (21,7%) – Importante 1 (4,3 %) – Moderadamente Importante
Jornalista e Professor	2	1 (4,3 %) – Extremamente Importante 1 (4,3 %) – Importante
Especialista em Tecnologia da Informação	2	2 (8,7%) – Extremamente Importante
Especialista em Segurança Cibernética	1	1 (4,3 %) – Extremamente Importante
Pós-graduando em Defesa Cibernética	1	1 (4,3 %) – Extremamente Importante
Doutora em Ciências Navais	1	1 (4,3 %) – Extremamente Importante
Mestre em Ciências Políticas	1	1 (4,3 %) – Importante
Mestre em Defesa Nacional	1	1 (4,3 %) – Extremamente Importante

PERFIL PROFISSIONAL	Frequência	Relevância
Especialista em psicologia militar	1	1 (4,3 %) – Extremamente Importante
Professor em Ciências da Computação	1	1 (4,3 %) – Extremamente Importante
Doutor (a) em Ciências Políticas	2	1 (4,3 %) – Extremamente Importante 1 (4,3 %) – Importante

Fonte: Elaborado pela autora

6.3 Terceira pergunta

A análise das respostas revela que a maioria dos respondentes acredita no uso direcionado das redes sociais para influenciar crenças, pensamentos e atitudes. A maior parte (52,1%; 12) concorda totalmente com a ideia de que houve uma engenharia intencional por trás da propagação de notícias falsas, formação de bolhas informacionais, manipulação dos usuários por meio de algoritmos e promoção de discursos de ódio que culminaram nos atos de 8 de Janeiro de 2023, em Brasília (DF). O resultado sugere uma forte aderência ao que foi apresentado na literatura sobre o uso combinado de estratégia política e ciências de dados nas redes sociais, como o relatório da Comissão Parlamentar Mista de Inquérito (CPMI).

Uma parcela menor, mas ainda substancial (21,7%; 5), concorda parcialmente sobre a influência das redes sociais nos eventos citados, mas acredita que as ações violentas não foram planejadas e sim aconteceram como resultado do próprio funcionamento do ecossistema digital. A mesma proporção (21,7%; 5) expressa neutralidade em relação à questão, indicando uma ausência de opinião clara sobre o impacto das redes sociais na disseminação de notícias falsas no referido evento.

Apenas um especialista (4,3%) discorda parcialmente da existência de uma engenharia intencional por trás da disseminação de notícias falsas e discursos de ódio. Apesar de reconhecer alguma influência das redes sociais, ele não acredita que tenha sido significativa. Ninguém discordou totalmente das conclusões da CPMI, o que sugere que a ideia de uma arquitetura planejada não foi rejeitada por nenhum dos participantes.

Tabela 6 – Análise quantitativa das respostas da 3ª pergunta, por concordância

ENUNCIADO: No livro Os Engenheiros do Caos (2019), Giuliano Da Empoli aponta evidências consistentes de que a propagação de notícias falsas e teorias da conspiração com o intuito de disseminar ódio, medo e influenciar eleições é um processo meticulosamente planejado, caracterizado como uma "obra de engenharia", e não simplesmente uma disfunção do ecossistema digital. A Comissão Parlamentar Mista de Inquérito (CPMI) instaurada no Congresso Nacional para investigar os atos de 8 de Janeiro de 2023, concluiu que houve influência das redes sociais na disseminação de notícias falsas, na formação de bolhas informacionais, na manipulação dos usuários por meio de algoritmos e na promoção de discursos de ódio.

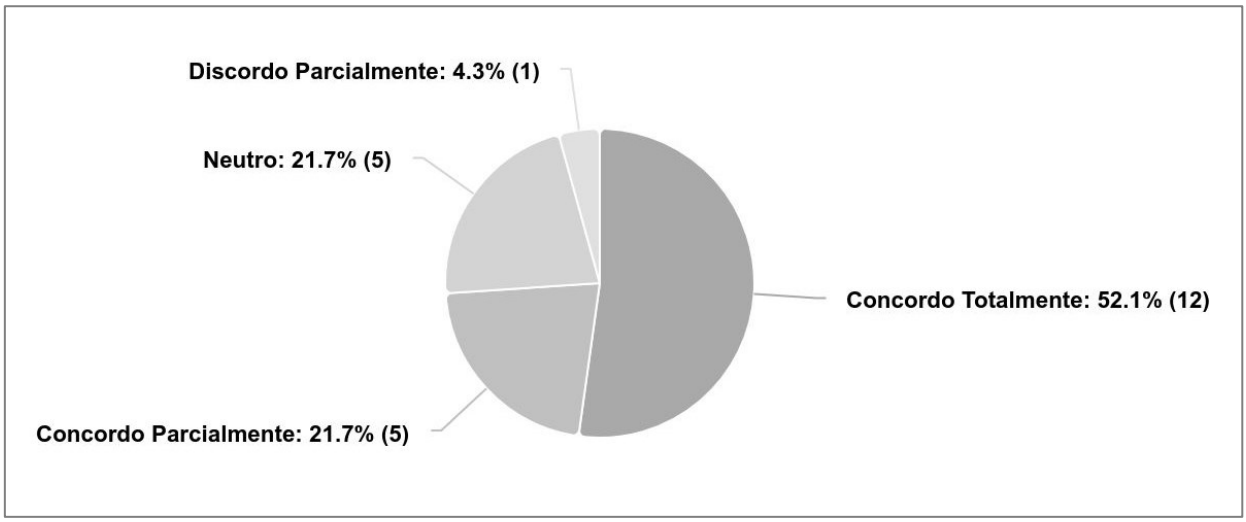
DA EMPOLI, Giuliano. Os engenheiros do caos. 1. ed. São Paulo: Vestígio, 2019.

CONGRESSO NACIONAL. Comissão Parlamentar Mista de Inquérito dos Atos de 8 de Janeiro de 2023. *Relatório final*. Brasília: Senado Federal, 2023. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9484688&ts=1697682413143&disposition=inline. Acesso em: 7 jan. 2024.

ALTERNATIVAS	Frequência	Percentual
Concordo Totalmente: Houve uma engenharia intencional por trás da propagação de notícias falsas, formação de bolhas informacionais, na manipulação dos usuários por meio de algoritmos e na promoção de discursos de ódio.	12	52,1%
Concordo Parcialmente: Houve uma influência significativa das redes sociais nos atos de 8 de janeiro, mas não foi planejada meticulosamente e sim resultado do próprio ecossistema interativo dessas plataformas.	5	21,7%
Neutro: Não tenho uma opinião clara sobre o impacto das redes sociais na disseminação de notícias falsas, que levaram aos atos de 8 de janeiro.	5	21,7%
Discordo Parcialmente: As redes sociais podem ter alguma influência, mas não tiveram um papel mais significativo na disseminação de desinformação e discursos de ódio.	1	4,3%
Discordo Totalmente: As conclusões da CPMI sobre a engenharia por trás da disseminação de notícias falsas são irreais; as redes sociais não tiveram impacto significativo nesse contexto.	0	0%

Fonte: Elaborado pela autora

Gráfico 3 – Representação visual dos resultados da 3ª pergunta



Fonte: Elaborado pela autora.

Tabela 7 – Análise das respostas da 3ª pergunta, por perfil profissional

PERFIL PROFISSIONAL	Frequência	Percentual
Oficial Superior das Forças Armadas	10	5 (21,7%) - Neutro 4 (17,3%) - Concordo Totalmente 1 (4,34%) - Discordo Parcialmente
Jornalista e Professor	2	2 (8,6%) - Concordo Totalmente
Especialista em Tecnologia da Informação	2	2 (8,6%) - Concordo Totalmente
Doutor (a) em Ciências Políticas	2	2 (8,6%) - Concordo Totalmente
Especialista em Segurança Cibernética	1	1 (4,3%) - Concordo Parcialmente
Pós-graduando em Defesa Cibernética	1	1 (4,3%) - Concordo Parcialmente
Doutora em Ciências Navais	1	1 (4,3%) - Concordo Parcialmente
Mestre em Ciências Políticas	1	1 (4,3%) - Concordo Parcialmente
Mestre em Defesa Nacional	1	1 (4,3%) - Concordo Parcialmente
Especialista em psicologia militar	1	1 (4,3%) - Concordo Parcialmente
Professor em Ciências da Computação	1	1 (4,3%) - Concordo Parcialmente

Fonte: Elaborado pela autora.

6.4 Quarta pergunta

A maioria reconheceu que as redes sociais podem ser utilizadas para enfraquecer a coesão social e fragilizar a confiança nas instituições governamentais. Esse resultado aponta para uma preocupação predominante com o impacto do uso malicioso dessas plataformas na estabilidade interna e na governança do país. Com 95,65% de adesão, o resultado da alternativa 1 demonstra um forte consenso entre a maior parte dos respondentes.

As afirmativas três e quatro apresentaram a mesma porcentagem de concordância, (78,3%), sugerindo que há uma percepção significativa de que as redes sociais podem ser utilizadas para distorcer a veracidade dos fatos. A segunda afirmativa obteve um pouco menos de adesão (73,9%), mas ainda revela uma percepção significativa de que as redes sociais podem afetar as relações internacionais e interesses econômicos e políticos do país. A quinta afirmativa com a menor adesão (56,5%) sugere que menos da metade dos respondentes concorda que as redes sociais aumentam a vulnerabilidade do país a outras formas de agressão.

Tabela 8 – Análise quantitativa das respostas da 4ª pergunta, por percentual

ENUNCIADO: A Expressão Psicossocial é um dos cinco aspectos pelos quais o Poder Nacional se manifesta nos ambientes externo e interno, segundo a Escola Superior de Guerra (2019), e está relacionada à formação da opinião pública e à disseminação de informações. Considerando que a influência das redes sociais na guerra cognitiva é significativa, pois pode moldar a maneira como as pessoas se identificam como cidadãos de um determinado país, como se relacionam entre si e como são percebidos pelo mundo, qual(is) afirmativas relacionadas à Expressão Psicossocial do Poder Nacional podem ser consideradas verdadeiras?

ESG - ESCOLA SUPERIOR DE GUERRA. *Fundamentos do poder nacional.* Rio de Janeiro: ESG, 2019.

ALTERNATIVAS	Frequência	Percentual
1- As redes sociais podem ser empregadas na guerra cognitiva para enfraquecer a coesão social e erodir a confiança nas instituições governamentais, promovendo narrativas negativas sobre o país.	22	95,65%
2 - As redes sociais podem ser utilizadas na guerra cognitiva para dificultar as relações do país com outros países e prejudicar seus interesses econômicos e políticos.	17	73,9%
3 - As redes sociais podem ser utilizadas na guerra cognitiva para distorcer a percepção internacional do país, construindo uma imagem prejudicial e minando suas relações diplomáticas e comerciais.	18	78,3%

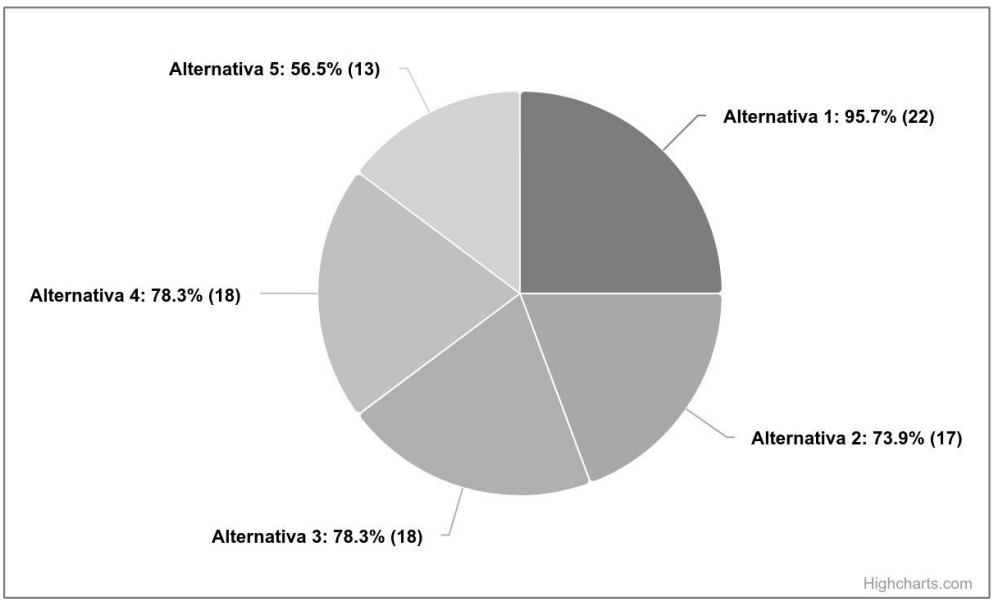
ENUNCIADO: A Expressão Psicossocial é um dos cinco aspectos pelos quais o Poder Nacional se manifesta nos ambientes externo e interno, segundo a Escola Superior de Guerra (2019), e está relacionada à formação da opinião pública e à disseminação de informações. Considerando que a influência das redes sociais na guerra cognitiva é significativa, pois pode moldar a maneira como as pessoas se identificam como cidadãos de um determinado país, como se relacionam entre si e como são percebidos pelo mundo, qual(is) afirmativas relacionadas à Expressão Psicossocial do Poder Nacional podem ser consideradas verdadeiras?

ESG - ESCOLA SUPERIOR DE GUERRA. *Fundamentos do poder nacional.* Rio de Janeiro: ESG, 2019.

ALTERNATIVAS	Frequência	Percentual
4 - As redes sociais podem ser utilizadas na guerra cognitiva para minar a coesão social e a legitimidade do governo nacional.	18	78,3%
5 - As redes sociais podem ser utilizadas na guerra cognitiva para tornar o país mais vulnerável a outras formas de agressão, como ataques militares ou cibernéticos.	13	56,5%

Fonte: Elaborado pela autora

Gráfico 4 – Representação visual dos resultados da 4ª pergunta



Fonte: Elaborado pela autora

Tabela 9 – Análise das respostas da 4ª pergunta, por perfil profissional

ALTERNATIVAS	Perfil Profissional	Percentual
1- As redes sociais podem ser empregadas na guerra cognitiva para enfraquecer a coesão social e erodir a confiança nas instituições governamentais, promovendo narrativas negativas sobre o país.	– Especialista em Segurança Cibernética – Jornalista e professor – Especialista em Tecnologia da Informação – Oficial Superior das Forças Armadas – Pós-graduando em Defesa Cibernética – Doutora em Ciências Navais – Doutor em Ciências Políticas – Mestre em Ciências Políticas – Mestre em Defesa Nacional – Professor na área de Tecnologia da Informação – Especialista em psicologia militar	– 1 (4,3%) – 2 (8,7%) – 2 (8,7%) – 9 (39,1%) – 1 (4,3%) – 1 (4,3%) – 1 (4,3%) – 1 (4,3%) – 0 (0,0%) – 1 (4,3%) – 1 (4,3%)
2 -As redes sociais podem ser utilizadas na guerra cognitiva para dificultar as relações do país com outros países e prejudicar seus interesses econômicos e políticos.	– Especialista em Segurança Cibernética – Jornalista e professor – Especialista em Tecnologia da Informação – Oficial Superior das Forças Armadas – Pós-graduando em Defesa Cibernética – Doutora em Ciências Navais – Doutor em Ciências Políticas – Mestre em Ciências Políticas – Mestre em Defesa Nacional – Professor na área de Tecnologia da Informação – Especialista em psicologia militar	– 1 (4,3%) – 2 (8,7%) – 1 (4,3%) – 7 (30,4%) – 1 (4,3%) – 1 (4,3%) – 1 (4,3%) – 1 (4,3%) – 1 (4,3%) – 0 (0,0%) – 1 (4,3%)
3 -As redes sociais podem ser utilizadas na guerra cognitiva para distorcer a percepção internacional do país, construindo uma imagem prejudicial e minando suas relações diplomáticas e comerciais.	– Especialista em Segurança Cibernética – Jornalista e professor – Especialista em Tecnologia da Informação – Oficial Superior das Forças Armadas – Pós-graduando em Defesa Cibernética – Doutora em Ciências Navais – Doutor em Ciências Políticas – Mestre em Ciências Políticas – Mestre em Defesa Nacional – Professor na área de Tecnologia da Informação – Especialista em psicologia militar	– 1 (4,3%) – 1 (4,3%) – 1 (4,3%) – 7 (30,4%) – 1 (4,3%) – 1 (4,3%) – 2 (8,7%) – 1 (4,3%) – 1 (4,3%) – 1 (4,3%) – 1 (4,3%)
4 - As redes sociais podem ser utilizadas na guerra cognitiva para minar a coesão social e a legitimidade do governo nacional.	– Especialista em Segurança Cibernética – Jornalista e professor – Especialista em Tecnologia da Informação – Oficial Superior das Forças Armadas – Pós-graduando em Defesa Cibernética – Doutora em Ciências Navais – Doutor em Ciências Políticas – Mestre em Ciências Políticas – Mestre em Defesa Nacional – Professor na área de Tecnologia da Informação – Especialista em psicologia militar	– 1 (4,3%) – 1 (4,3%) – 1 (4,3%) – 7 (30,4%) – 1 (4,3%) – 1 (4,3%) – 2 (8,7%) – 1 (4,3%) – 1 (4,3%) – 1 (4,3%) – 1 (4,3%)

ALTERNATIVAS	Perfil Profissional	Percentual
5 - As redes sociais podem ser utilizadas na guerra cognitiva para tornar o país mais vulnerável a outras formas de agressão, como ataques militares ou cibernéticos.	– Especialista em Segurança Cibernética – Jornalista e professor – Especialista em Tecnologia da Informação – Oficial Superior das Forças Armadas – Pós-graduando em Defesa Cibernética – Doutora em Ciências Navais – Doutor em Ciências Políticas – Mestre em Ciências Políticas – Mestre em Defesa Nacional – Professor na área de Tecnologia da Informação – Especialista em psicologia militar	– 1 (4,3%) – 1 (4,3%) – 1 (4,3%) – 6 (26,1%) – 1 (4,3%) – 1 (4,3%) – 0 (0,0%) – 0 (0,0%) – 1 (4,3%) – 0 (0,0%) – 1 (4,3%)

Fonte: Elaborado pela autora.

6.5 Quinta pergunta

A educação e a conscientização foram escolhidas pela maioria absoluta dos entrevistados (100%) como fundamentais para combater a guerra cognitiva. Esse resultado demonstra um consenso sobre a importância da literacia digital como estratégia para preparar a população contra as campanhas de desinformação, sendo essencial para que a sociedade possa identificar e se proteger contra as ameaças da manipulação cognitiva.

Outras medidas apontadas pelos respondentes como importantes foram o combate às *fake news* (65,2%) e a necessidade de uma resposta rápida (56,5%) às campanhas de desinformação nas redes sociais. Esses números refletem uma preocupação importante com a disseminação de notícias falsas, o que demonstra que muitos reconhecem a urgência de agir rapidamente para mitigar os impactos desse novo tipo de guerra.

As parcerias com plataformas de rede social (47,8%) e o engajamento com a comunidade online (43,5%) também foram consideradas medidas importantes, indicando uma necessidade de estabelecer parcerias para a criação conjunta de estratégias contra a desinformação, promovendo a divulgação de informações precisas e o debate construtivo.

Os participantes tiveram, ainda, a oportunidade de compartilhar suas opiniões, percepções ou experiências de forma livre e detalhada em um campo específico do questionário. Os respondentes abordaram diversos pontos relacionados à manipulação cognitiva nas redes sociais, Os respondentes abordaram temas como a vulnerabilidade psicossocial causada pela manipulação de informações, os riscos das IAs generativas na criação de narrativas falsas, as motivações variadas por trás da disseminação de desinformação, e a necessidade de regulação

das plataformas digitais. Também foi destacada a importância de incorporar o combate à desinformação em uma Estratégia Nacional de Segurança e a proposta de seminários e fóruns para aumentar a conscientização pública.

– **Vulnerabilidade sistêmica na esfera psicossocial:** O primeiro respondente, um professor da área de Tecnologia da Informação, aponta que mesmo informações verdadeiras, quando divulgadas em um contexto de violência, podem prejudicar negativamente o aspecto psicossocial. Ele mencionou que os problemas econômicos também têm o mesmo efeito sobre o indivíduo, aumentando essa influência.

– **Evolução das IAs generativas:** O mesmo respondente alerta para os riscos emergentes do uso das inteligências artificiais generativas na criação de narrativas. Ele também destaca o risco de "alucinações" geradas pelas IA, que podem criar documentos falsos para provar uma afirmação fabricada e potencializar a manipulação online.

– **Motivações dos disseminadores de desinformação:** Ele também ressalta que nem todo aquele que dissemina desinformação tem o objetivo de desestabilizar o país ou enganar. Alguns agem assim por fama ou dinheiro, enquanto outros acreditam na informação falsa como se fosse verdadeira. Essa observação aborda a complexidade das motivações por trás da desinformação e sugere que abordagens abrangentes para a combater.

– **Regulação das plataformas digitais:** Um outro respondente, também da área de Tecnologia da Informação, propôs como medidas necessárias a regulação democrática das plataformas digitais e a criminalização dos agentes que lucram com a desinformação. Além disso, ele destaca a necessidade de investimentos em soberania digital nacional para a criação de plataformas e redes públicas nacionais em substituição às redes digitais estrangeiras.

– **Integração em uma Estratégia Nacional de Segurança:** Um oficial das Forças Armadas enfatiza a importância de incorporar ações de combate à desinformação em uma Estratégia Nacional de Segurança. Ele também salienta a necessidade de que essa estratégia contemple o fortalecimento da identidade nacional, do patriotismo e da conexão da população com o Estado.

– **Criação de Seminários e Fóruns:** O último respondente, pós-graduando em Defesa Cibernética, entende que a educação e a discussão pública ajudam a aumentar a conscientização sobre os desafios ligados à desinformação e à manipulação social. Para isso, ele propõe seminários e fóruns como espaços para discutir geopolítica, persuasão e métodos de poder.

Tabela 10 – Análise quantitativa das respostas da 5ª pergunta, por percentual

ENUNCIADO: O uso cada vez mais intenso das redes sociais como ferramenta de guerra cognitiva tem sido percebido em escala global. Exemplos como os da China, em Taiwan, e Rússia, na Ucrânia, têm sido objeto de estudo e acompanhamento por especialistas da área de Defesa de diversas nacionalidades (Nichols; Corrêa, 2023). Indique a(s) medida(s) fundamental(is) para que o Estado brasileiro esteja preparado diante de uma eventual guerra cognitiva empregada por agentes externos.

NICHOLS, Giselli C.L.; CORRÊA, Claudio R. A guerra cognitiva nas redes sociais e suas implicações para a segurança dos Estados. Revista da ESG, Rio de Janeiro, v. 28, n. 1, p. 1-10, jan./jun. 2023. Disponível em: https://revista.esg.br/index.php/revistadaesg/article/view/1297/1072. Acesso em 7 jan. 2024.

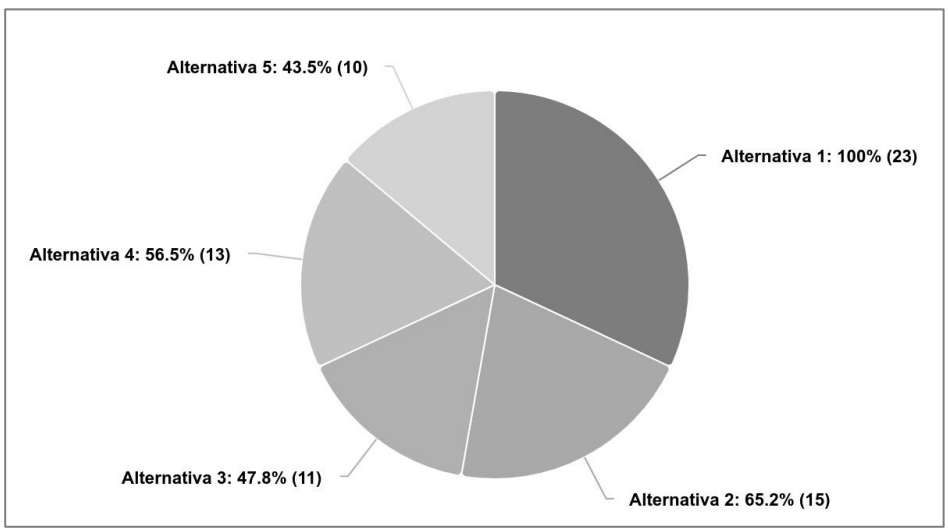
ALTERNATIVAS	**Frequência**	**Percentual**
Combate às fake news: Utilizar ferramentas de monitoramento e análise para rastrear a disseminação de informações falsas e identificar padrões de comportamento suspeito nas redes sociais.	15	65,2%
Educação e conscientização: Promover a alfabetização digital e a conscientização sobre a disseminação de informações falsas, capacitando as pessoas a identificar e questionar fontes duvidosas.	23	100%
Parcerias com plataformas de mídia social: Trabalhar em conjunto com as principais plataformas de mídia social para desenvolver e implementar políticas e tecnologias que limitem a propagação de desinformação.	11	47,8%
Resposta rápida: Desenvolver capacidades de resposta rápida para desmentir informações falsas e fornecer informações precisas em tempo hábil.	13	56,5%
Engajamento com a comunidade online: Estabelecer diálogo para promover a divulgação de informações precisas e construir resiliência contra a desinformação.	10	43,5%
Acréscimos realizados pelos respondentes		

- A vulnerabilidade na esfera psicossocial (como noutras esferas) é sistêmica. Neste sentido, com a população sendo alvo de violência, mesmo informações verdadeiras sendo disseminadas prejudicam o psicossocial. Similar com os problemas econômicos.
- Outro problema reside na possibilidade de se criar narrativas falsas a partir de informações verdadeiras, algo que ultrapassa o conceito usual de *fake news*. Neste caso, o trabalho de engenharia é muito mais avançado e difícil de rastrear.
- É preciso atentar para as evoluções nas IAs generativas, que permitem a criação de todo tipo de narrativa e as próprias empresas, em seus documentos, apresentam os riscos de alucinações, quando a IA cria até os documentos para provar o que afirma.

Acréscimos realizados pelos respondentes
– Nem todos os disseminadores de desinformação operam com fins de desestabilizar o país ou enganar, alguns operam simplesmente para ganhar fama ou dinheiro e há quem acredite que a notícia falsa que dissemina é verdadeira – Em alguns desses casos, é preciso ir além da "educação", pois se trata de problemas psicológicos. – Devem ocorrer duas regulações: Empresas de mídias sociais e empresas de IA; e as empresas de mídias sociais (Meta, X, Tiktok entre outras). A soma dos dois ambientes (Mídias sociais com IA, em especial Visão Computacional e IA Generativa) possui um potencial devastador para gerar desinformação e desestabilizar o tecido social. – Respondente: Professor na área de Tecnologia da Informação
– Regulação democrática das plataformas digitais; criminalização dos principais agentes que lucram com a desinformação socialmente nefasta (antidemocrática, negacionista, que incita a violência contra minorias etc.); investimento em soberania digital nacional, criação de plataformas e redes públicas nacionais, acabando com a dependência de nuvens e redes digitais estrangeiras. – Respondente: Especialista em Tecnologia da Informação
– Qualquer medida dessa natureza só faz sentido se integrante de uma Estratégia Nacional de Segurança, onde a Defesa seja uma das vertentes da Segurança. – Nesse contexto, fortalecimento da identidade nacional, do sentimento de patriotismo e da identificação do povo com o Estado. – Respondente: Oficial Superior das Forças Armadas
– Criação de Seminários e Fóruns sobre Geopolítica, Persuasão e Técnicas de Poder e Manipulação Social. – Respondente: Pós-graduando em Defesa Cibernética

Fonte: Elaborado pela autora.

Gráfico 5 – Representação visual dos resultados da 5ª pergunta



Fonte: Elaborado pela autora.

Tabela 11 – Análise das respostas da 5ª pergunta, por perfil profissional

ALTERNATIVAS	Perfil Profissional	Porcentagem
1 - Combate às fake news: Utilizar ferramentas de monitoramento e análise para rastrear a disseminação de informações falsas e identificar padrões de comportamento suspeito nas redes sociais.	– Especialista em Segurança Cibernética – Jornalista e professor – Especialista em Tecnologia da Informação – Oficial Superior das Forças Armadas – Pós-graduando em Defesa Cibernética – Doutora em Ciências Navais – Doutor(a) em Ciências Políticas – Mestre em Ciências Políticas – Mestre em Defesa Nacional – Professor na área de Tecnologia da Informação – Especialista em psicologia militar	– 1 (4,3%) – 2 (8,7%) – 2 (8,7%) – 4 (17,4%) – 1 (4,3%) – 1 (4,3%) – 2 (8,7%) – 0 (0%) – 1 (4,3%) – 0 (0%) – 1 (4,3%)
2 - Educação e conscientização: Promover a alfabetização digital e a conscientização sobre a disseminação de informações falsas, capacitando as pessoas a identificar e questionar fontes duvidosas.	–Especialista em Segurança Cibernética –Jornalista e professor –Especialista em Tecnologia da Informação –Oficial Superior das Forças Armadas –Pós-graduando em Defesa Cibernética –Doutora em Ciências Navais –Doutor(a) em Ciências Políticas –Mestre em Ciências Políticas –Mestre em Defesa Nacional –Professor na área de Tecnologia da Informação –Especialista em psicologia militar	– 1 (4,3%) – 2 (8,7%) – 2 (8,7%) – 8 (34,7%) – 1 (4,3%) – 1 (4,3%) – 2 (8,7%) – 1 (4,3%) – 1 (4,3%) – 1 (4,3%) – 1 (4,3%)
3 - Parcerias com plataformas de mídia social: Trabalhar em conjunto com as principais plataformas de mídia social para desenvolver e implementar políticas e tecnologias que limitem a propagação de desinformação.	–Especialista em Segurança Cibernética –Jornalista e professor –Especialista em Tecnologia da Informação –Oficial Superior das Forças Armadas –Pós-graduando em Defesa Cibernética –Doutora em Ciências Navais –Doutor(a) em Ciências Políticas –Mestre em Ciências Políticas –Mestre em Defesa Nacional –Professor na área de Tecnologia da Informação –Especialista em psicologia militar	– 1 (4,3%) – 2 (8,7%) – 1 (4,3%) – 3 (13%) – 0 (0%) – 0 (0%) – 1 (4,3%) – 0 (0%) – 1 (4,3%) – 0 (0%) – 1 (4,3%)
4 - Resposta rápida: Desenvolver capacidades de resposta rápida para desmentir informações falsas e fornecer informações precisas em tempo hábil.	– Especialista em Segurança Cibernética – Jornalista e professor – Especialista em Tecnologia da Informação – Oficial Superior das Forças Armadas – Pós-graduando em Defesa Cibernética – Doutora em Ciências Navais	– 0 (0%) – 1 (4,3%) – 1 (4,3%) – 7 (30,4%) – 1 (4,3%) – 1 (4,3%)

	– Doutor(a) em Ciências Políticas – Mestre em Ciências Políticas – Mestre em Defesa Nacional – Professor na área de Tecnologia da Informação – Especialista em psicologia militar	– 1 (4,3%) – 0 (0%) – 1 (4,3%) – 0 (0%) – 1 (4,3%)
5 - Engajamento com a comunidade online: Estabelecer diálogo para promover a divulgação de informações precisas e construir resiliência contra a desinformação.	– Especialista em Segurança Cibernética – Jornalista e professor – Especialista em Tecnologia da Informação – Oficial Superior das Forças Armadas – Pós-graduando em Defesa Cibernética – Doutora em Ciências Navais – Doutor(a) em Ciências Políticas – Mestre em Ciências Políticas – Mestre em Defesa Nacional – Professor na área de Tecnologia da Informação – Especialista em psicologia militar	– 0 (0%) – 0 (0%) – 1 (4,3%) – 3 (0%) – 1 (4,3%) – 1 (4,3%) – 1 (4,3%) – 1 (4,3%) – 1 (4,3%) – 0 (0%) – 1 (4,3%)

Fonte: Elaborado pela autora.

5.4 CONSIDERAÇÕES FINAIS SOBRE OS RESULTADOS DA SURVEY

Do ponto de vista geral dos pesquisados, a guerra cognitiva nas redes sociais representa um desafio cada vez mais complexo e em rápida mudança. Seu dinamismo e alcance no mundo contemporâneo vão além das fronteiras físicas e do tempo. Em uma realidade onde a desinformação e as *fake news* podem se espalhar rapidamente e atingir um público massivo e global, a resposta a essas ameaças precisa ser igualmente rápida e abrangente.

A pesquisa *survey* possibilitou *insights* e análises específicas da guerra cognitiva no contexto brasileiro das redes sociais. Ao olhar para as sutilezas e características especiais desse fenômeno, o estudo ajudou a identificar fundamentos para a formulação de políticas públicas e estratégias de defesa adaptadas às necessidades e desafios do país.

No entanto, enfrentar efetivamente a guerra cognitiva requer mais do que apenas compreensão teórica e análise acadêmica. Neste sentido, a *survey* ratificou os entendimentos, identificados na revisão da literatura, de que é fundamental envolver ativamente uma variedade de atores sociais, incluindo governos, instituições acadêmicas, empresas privadas e a sociedade civil, em um esforço colaborativo e coordenado. Somente através dessa colaboração ampla e inclusiva será possível reunir experiências, práticas, recursos e perspectivas necessárias para desenvolver e implementar políticas públicas e estratégias de defesa verdadeiramente eficazes.

Uma abordagem bem coordenada permite que diferentes partes da sociedade trabalhem cooperativamente, o que abrange detectar e combater campanhas de desinformação e construir uma cultura de conscientização e resistência digital. Por meio desse amplo trabalho em equipe, é possível reforçar as defesas contra os efeitos negativos das guerras cognitivas, protegendo a informação nas redes sociais e mantendo a estabilidade da democracia.

6 POLÍTICAS PÚBLICAS DE DEFESA NACIONAL: ANÁLISES INTEGRATIVAS E RECOMENDAÇÕES ESTRATÉGICAS

Em um mundo cada vez mais interconectado e dependente da informação, as ameaças ao Poder Nacional brasileiro assumem novas formas e desafiam as nações de maneiras inéditas (ESG, 2024). A guerra cognitiva, caracterizada pelo uso estratégico de informações e narrativas para manipular a percepção pública, influenciar comportamentos, desestabilizar e deslegitimar sistemas políticos e sociais, surge como uma das principais preocupações no cenário global contemporâneo (Cluzel, 2020).

No contexto brasileiro, a pesquisa sobre as ameaças da guerra cognitiva à Expressão Psicossocial do Poder Nacional se torna cada vez mais relevante para a defesa da soberania, da democracia e dos interesses nacionais. À medida que a tecnologia digital avança e as redes sociais ganham cada vez mais espaço na vida em sociedade, os desafios do Brasil com a manipulação de informações e influência digital aumentam consideravelmente. Essas táticas de guerra cognitiva podem abalar a estabilidade política e social, enfraquecer a confiança do público nas instituições democráticas e prejudicar a segurança nacional.

As iniciativas destacadas neste estudo – abrangendo áreas como inteligência, defesa, segurança da informação, ciência, tecnologia e inovação –, oferecem um arcabouço legal e estratégico essencial para o enfrentamento da guerra cognitiva. Por meio da análise crítica de soluções inovadoras, a pesquisa pôde contribuir significativamente para a construção de políticas públicas e de uma sociedade brasileira mais preparada para enfrentar os desafios virtuais do século XXI.

Diversos autores como Lazer (2018), Vosoughi, Roy, Aral (2018) e Wardle, Derakhshan (2018) apresentam abordagens abrangentes com estratégias para minimizar a propagação de desinformação online. Essas estratégias incluem a detecção de conteúdo enganoso através de análise de sentimentos e aprendizado de máquina; a contenção da desinformação por meio da identificação e remoção de contas suspeitas, e a limitação do compartilhamento e diminuição da exposição a informações falsas. Eles também ressaltam a necessidade da literacia digital para que a sociedade saiba identificar e lidar com conteúdo enganoso e a colaboração entre plataformas digitais; além do uso de tecnologias emergentes, como inteligência artificial, para aprimorar a detecção e o combate à guerra cognitiva nas redes sociais.

6.1 INICIATIVAS DE COMBATE À GUERRA COGNITIVA NAS REDES SOCIAIS

Conforme analisado até aqui, ainda que as redes sociais tenham se consolidado como um novo espaço para o debate público, permitindo que o compartilhamento de ideias e participação ativa dos cidadãos na vida cívica, elas também se tornaram um terreno fértil para a disseminação de desinformação e *fake news*, visando manipular a opinião pública e desestabilizar democracias. Nesse novo contexto, surgem desafios tanto para a governança digital quanto para a proteção da soberania informacional.

Uma dessas estratégias desafiadoras diz respeito às ações realizadas com o objetivo de influenciar ou manipular a informação em outro país, visando desestabilizar suas instituições, processos democráticos ou sociedade. Conhecida como *Foreign Information Manipulation and Interference (FIMI*), essa abordagem é utilizada por Estados, entidades privadas ou indivíduos para atingir objetivos políticos, econômicos, sociais ou militares, colocando em alerta governos em todo o mundo. Diversos países têm reconhecido a gravidade dessa ameaça e procurado implementar medidas para combatê-la, como a adoção de leis e regulamentações específicas, bem como o fortalecimento da segurança cibernética e a cooperação doméstica e internacional (G7, 2022).

Considerando essas questões, este capítulo se concentra em exemplos de iniciativas que visam fortalecer a resiliência da democracia no ambiente digital, além de apresentar subsídios para a elaboração de políticas públicas pertinentes no âmbito do Ministério da Defesa. Essas ações procuram proteger a integridade dos processos democráticos, garantir a transparência e a veracidade dos fatos na comunicação pública. Também procuram promover a segurança nacional e a estabilidade do país no contexto internacional. Embora não abordem especificamente a guerra cognitiva de maneira específica, essas iniciativas lidam com estratégias relevantes dessa dinâmica nas redes sociais.

6.1.1 Iniciativas da União Europeia (UE)

Considerando que a desinformação fragiliza a confiança nas instituições políticas democráticas e influencia cidadãos a apoiar ideias radicais e extremistas, a União Europeia (UE) iniciou, em 2014, esforços para criar uma política comum de combate às influências da informação externa na esfera política. Com esse objetivo, o Conselho Europeu começou a estruturar um plano de combate à campanha de desinformação empregada pela Rússia, que tem utilizado táticas de guerra cognitiva para influenciar e distorcer a percepção pública em diversos

países da UE. O ecossistema de influência russo foi identificado através de uma intensa análise de inteligência, que revelou a extensão das ações para fragilizar a estabilidade e a coesão dos países da União Europeia. Essas operações incluíram campanhas de desinformação coordenadas, atividades cibernéticas maliciosas e tentativas de influenciar diretamente processos políticos e sociais em países da União Europeia, conforme pode-se observar no texto a seguir:

> A maior ameaça para a UE provém da desinformação por parte da Federação da Rússia. Trata-se de uma prática sistemática, que dispõe de bastantes recursos e é efetuada numa escala diferente dos restantes países. Em termos de coordenação, níveis de definição dos alvos e implicações estratégicas, as ações de desinformação da Rússia inserem-se no âmbito de uma ameaça híbrida mais vasta, que recorre a diferentes ferramentas e alavancas, assim como a agentes não estatais (Comissão Europeia, 2018, p. 4).

O Grupo de Trabalho de Comunicação Estratégica para o Leste (*East StratCom),* criado pelo Serviço Europeu para a Ação Externa (SEAE), identificou que o número de casos de desinformação atribuídos a fontes russas mais que dobrou de 2018 para 2019, passando de 434 casos para 998 eventos registrados. A grande maioria deles foi observada na internet, considerada a principal fonte de notícias para 57% dos europeus. O *East StratCom* monitora e analisa a desinformação e propaganda russas direcionadas à UE e seus vizinhos orientais, desenvolvendo respostas estratégicas. Esse monitoramento abrange uma ampla gama de fontes, desde redes sociais até meios de comunicação tradicionais, permitindo uma compreensão abrangente das estratégias e táticas empregadas (European Parliament, 2019; Comissão Europeia, 2018).

Em 2018, a Comissão Europeia estabeleceu um Plano de Ação contra a Desinformação (PAD) para fornecer uma resposta coordenada e abrangente com o objetivo de proteger a sociedade. A proposta se baseou em quatro pilares principais: o aprimoramento das capacidades das instituições da União Europeia para detectar, analisar e denunciar a desinformação; o fortalecimento da coordenação e das respostas conjuntas à desinformação; o envolvimento do setor privado na luta contra a desinformação; e a conscientização e reforço da resiliência da sociedade (Comissão Europeia, 2018).

Para aprimorar as capacidades das instituições da União Europeia contra a desinformação, a Comissão Europeia incluiu algumas ações consideradas necessárias para a efetividade do plano. As principais orientações incluem o fortalecimento dos grupos de trabalho voltados para ameaças híbridas, a consolidação das equipes de comunicação estratégica, a

realização de investimentos em ferramentas analíticas, além da contratação de novos serviços para monitoramento da mídia. A cooperação entre equipes, incluindo campanhas de comunicação, realização de análises de risco e avaliação das informações, também foram consideradas fundamentais para o combate à desinformação (Comissão Europeia, 2018).

Partindo da premissa de que o combate eficaz às campanhas de desinformação depende das primeiras horas após seu surgimento, o PAD propõe a criação de um sistema de alerta rápido. Esse sistema seria capaz de identificar em tempo real o aparecimento dessas estratégias, fortalecendo assim a coordenação e as respostas conjuntas a essas ameaças. Com isso, seus formuladores esperam garantir uma reação mais ágil e eficaz para proteger a sociedade contra a desinformação. Essa infraestrutura tecnológica visa facilitar a troca de informações e a avaliação da situação, estabelecendo um entendimento comum, e permitindo a coordenação da resposta, a distribuição de tarefas e a utilização adequada dos recursos disponíveis (Comissão Europeia, 2018).

A Comissão também exortou as plataformas online, anunciantes e empresas de publicidade a participarem conjuntamente dessas iniciativas, em reconhecimento de que não só os esforços estatais são suficientes para o combate às campanhas de desinformação. O grupo percebeu que, embora algumas dessas plataformas tenham tomado medidas para combater a desinformação, essas iniciativas não foram suficientes para conter o problema (Comissão Europeia, 2018).

Reconhecendo essa brecha, e em resposta à necessidade de uma ação mais robusta, a Comissão publicou um código de conduta contra a desinformação em 2018. Esse código estabelece um conjunto de princípios e medidas que esses agentes devem seguir para combater a disseminação de informações falsas. O cumprimento dos compromissos pelos signatários é supervisionado pela Comissão, com o apoio do Grupo de Reguladores Europeus dos Serviços de Comunicação Social Audiovisual (ERGA). Caso os resultados não sejam satisfatórios, a Comissão se reserva o direito de propor novas medidas de caráter normativo, para garantir a efetividade das ações (Comissão Europeia, 2018).

A Comissão entende também que enfrentar a desinformação de forma global exige um esforço conjunto que vai além de governos e plataformas online. A sociedade civil, composta por diversos grupos e organizações, tem um papel fundamental a desempenhar nesse processo, especialmente no contexto político e eleitoral. Neste sentido, o PDA previu ações de sensibilização para aumentar a transparência das eleições e reforçar a confiança nesses processos por meio da literacia midiática. Uma das ações prevê o apoio a campanhas de informação para orientar os usuários sobre como se proteger contra os riscos que as novas

tecnologias, como as *deepfakes*, podem representar. Da mesma forma, o órgão entende que a participação dos meios de comunicação independentes e de jornalistas investigativos é vital na denúncia de campanhas de desinformação (Comissão Europeia, 2018).

Em relação ao problema da desinformação nos meios de comunicação convencionais, Wardle e Derakhshan (2017) destacam um elemento importante para a questão. Eles advertem que a mídia pode, sem querer, intensificar conteúdo falso ou enganoso. Essa situação pode ocorrer de várias formas, incluindo a divulgação de conteúdo não verificado e que não corresponda aos fatos. Esse compartilhamento de informações de maneira imprecisa e sem o devido contexto pode levar a interpretações equivocadas e à disseminação de desinformação. Além disso, ao dar espaço a vozes extremistas ou marginais, os veículos de comunicação concedem visibilidade a indivíduos ou grupos que promovem desinformação e narrativas enganosas. Devido à credibilidade desses meios oficiais, essa exposição sugere uma aparência de legitimidade às ideias desses sujeitos, ampliando sua influência e alcance.

Essa questão, no entanto, é rebatida por Schudson (2017). Ele defende que "um jornalista responsável não produz notícias falsas, nem notícias exageradas ou notícias corrompidas. Não subordina o relato honesto à coerência ideológica ou ao ativismo político", mas obedece a regras profissionais pré-estabelecidas como "colocar a verdade em primeiro lugar". A disseminação de *fake news*, portanto, não é a prática do jornalismo ético e comprometido com a verdade dos fatos.

6.1.2 Iniciativas do Governo da Espanha

Em 2020, o Governo da Espanha reuniu especialistas da sociedade civil, representantes do setor acadêmico, privado e da administração pública com o objetivo de gerar conhecimento sobre o desafio das campanhas de desinformação. Essa iniciativa procurou o alinhamento com a estratégia da União Europeia para enfrentar essa ameaça crescente. A cooperação público-privada foi promovida pelo Departamento de Segurança Nacional (DSN) espanhol. As iniciativas do governo da Espanha contra a desinformação complementam as políticas da UE, abordando desafios específicos do país e garantindo uma resposta abrangente e eficaz à desinformação em níveis nacional e supranacional. Elas são baseadas no entendimento de que o pleno exercício da democracia requer, acima de tudo, um ambiente que promova o respeito às liberdades de pensamento, informação e expressão, que são os princípios fundamentais para o fortalecimento da sociedade democrática e para a garantia de um ambiente digital saudável e inclusivo (DSN, 2022).

Diante dos riscos significativos para a estabilidade e segurança nacional, a Espanha reconheceu a necessidade de incluir as campanhas de desinformação como uma ameaça prioritária a ser enfrentada na sua Estratégia Nacional de Segurança de 2021. Essa decisão indica uma crescente preocupação com os impactos negativos da desinformação em larga escala sobre a integridade dos processos políticos e a coesão social (DSN, 2022).

A maioria desses trabalhos adota uma abordagem conceitual e informativa, com o propósito de aprofundar a compreensão sobre o fenômeno. Um dos direcionamentos visa avaliar o quadro regulatório relacionado à desinformação, especialmente no contexto da segurança nacional, o que é fundamental para entender como as políticas públicas podem ser aprimoradas para enfrentar essa ameaça (DSN, 2022).

Como apontado no estudo de 2022 do DSN, o Estado espanhol reconhece o potencial transformador da era digital para a democracia, particularmente no que se refere ao acesso à informação. As plataformas online e redes sociais são vistas como ferramentas valiosas para o livre intercâmbio de ideias, debates construtivos e engajamento cívico. No entanto, essa transformação também revela vulnerabilidades significativas.

A facilidade com que informações são compartilhadas virtualmente, muitas vezes sem verificação adequada, criou um ambiente propício para a propagação de desinformação e manipulação, representando uma ameaça não somente aos processos democráticos, mas também à segurança nacional, conforme é abordado no texto a seguir:

> As campanhas de desinformação, no campo da segurança nacional, são entendidas como padrões de comportamento desenvolvidos no domínio da informação, realizados de forma coordenada e intencional, cuja implementação e disseminação representam ameaça aos valores constitucionais, aos processos democráticos, às instituições democraticamente constituídas e, portanto, à segurança nacional (DSN, 2022, p. 7, tradução nossa)[34].

O estudo em questão aponta que, no contexto da segurança nacional, as campanhas de desinformação se configuram como padrões de comportamento intencional e coordenado, direcionadas para manipular a opinião pública e influenciar decisões estratégicas. Sua disseminação representa um ataque direto aos valores democráticos, às instituições do Estado e à segurança nacional. Essa ameaça não se limita a ações de usuários individuais, mas se

[34] *"Las campañas de desinformación, en el ámbito de la seguridad nacional son entendidas como patrones de comportamiento desarrollados en el dominio informativo, llevados a cabo de forma coordinada e intencional, cuya implantación y difusión supone una amenaza para los valores constitucionales, los procesos democráticos, las instituciones democráticamente constituidas y, por ende, para la seguridad nacional".*

expande para campanhas orquestradas por governos estrangeiros e agentes privados, (DSN, 2022, p. 52, tradução nossa)[35]: "A desinformação e a interferência estrangeiras podem ser realizadas por governos estrangeiros ou por atores não estatais estrangeiros, incluindo elementos que estão direta e publicamente ligados, financiados e controlados por eles".

Dois anos depois, a UE voltou a sublinhar a desinformação no Plano de Ação para a Democracia Europeia (EDAP, na sigla em inglês). Em dezembro de 2020, a entidade alertou os Estados-Membros para o risco representado pelas campanhas maliciosas, tanto para a segurança das instituições europeias e a dos Estados-Membros, bem como contra a integridade dos valores e processos democráticos em toda a Europa (DSN, 2022).

Um dos pontos destacados pelos 39 especialistas multidisciplinares que participaram do estudo foi a importância de estabelecer uma linguagem comum e uma compreensão compartilhada do problema para que a formulação de políticas públicas seja mais eficiente e abrangente. Isso é importante porque, quando diferentes agentes (governos, organizações, sociedade civil etc.) usam termos e conceitos que não são claros ou que variam em significado, a comunicação se torna ineficaz (DSN, 2022).

Eles identificaram que o significado de *"fake news"* é um dos que mais traziam variação conceitual, apresentando sérias ambiguidades. Segundo os pesquisadores, a falta de consenso na definição dificulta a comunicação eficaz e sua compreensão precisa, tornando-o inadequado para abranger a complexa realidade do fenômeno. Esse fato é particularmente importante para casos de ações judiciais, cujos conceitos necessitam ser mais precisos e restritivos a fim de garantir que a justiça seja aplicada de forma equilibrada (DSN, 2022).

Além disso, a instrumentalização política do termo *fake news* acabou distorcendo seu significado original, gerando uma conotação negativa que impede uma análise mais imparcial do problema. Diante dessa constatação, muitos pesquisadores têm optado pelo termo "desinformação", considerado mais preciso e abrangente. Essa terminologia já foi adotada pela Comissão Europeia, que a define como "informações comprovadamente falsas ou enganosas, criadas, apresentadas e divulgadas com o propósito de gerar lucro ou de enganar deliberadamente o público, e que podem causar prejuízos à sociedade" (DNS, 2022, p. 47, tradução nossa)[36].

---

[35] *"La desinformación e interferencia extranjera puede ser llevada a cabo por gobiernos extranjeros o por actores extranjeros no estatales, incluidos los elementos que están directamente y públicamente vinculados, financiados y controlados por ellos".*

[36] *"información verificablemente falsa o engañosa que se crea, presenta y divulga con fines lucrativos o para inducir a error deliberadamente a la población, y que puede causar un perjuicio público."*

As principais propostas resultantes dos estudos abordam o desenvolvimento de procedimentos, ferramentas, fóruns e códigos de conduta para combater a desinformação. Essas medidas têm como objetivo proteger os sistemas democráticos e os interesses da segurança nacional. Para isso, foi desenvolvido um conjunto de sistemas voltados para a gestão de informações e inteligência de ameaças, conhecidos como OpenCTI, AMITT e STIX. (DSN, 2022).

O OpenCTI é uma plataforma de código aberto desenvolvida conjuntamente pela UE e a França para o gerenciamento de informações de inteligência que possam representar ameaças às organizações. Essas ameaças podem ser tanto cibernéticas quanto de desinformação e interferência. A plataforma permite que os usuários mesclem informações técnicas e não técnicas enquanto vinculam cada informação à sua fonte primária (DSN, 2022).

O AMITT *(Adversarial Misinformation and Influence Tactics and Techniques)* é uma estrutura analítica que usa práticas de segurança para entender incidentes de desinformação. Por meio de um conjunto de diretrizes e abordagens, fornece uma visão de como as campanhas de desinformação são executadas, identificando padrões de comportamento e técnicas utilizadas pelos adversários (DSN, 2022).

O STIX *(Structured Threat Information Expression)* é um padrão de linguagem que executa a troca de informações de ameaças cibernéticas de maneira estruturada, padronizada e interoperável, incluindo incidentes de desinformação. A principal finalidade dessa estrutura de código aberto é facilitar a colaboração entre pesquisadores, analistas de segurança, equipes de resposta a incidentes e outras partes interessadas, permitindo que compartilhem e analisem informações sobre ameaças de forma eficiente e consistente (DSN, 2022).

Um outro assunto de grande importância se refere a questões regulatórias. Os especialistas alertam para a sensibilidade do tema e consideram que é necessário evitar uma criminalização geral do fenômeno da desinformação, devido à grande dificuldade em defini-lo com a precisão necessária para que a regulação seja eficaz. Tal abordagem poderia resultar em abusos e limitações indevidas à liberdade de expressão. O grupo argumenta que muitas formas específicas, como crimes de ódio e calúnia, já são tratadas pela legislação existente. Além disso, entendem que os padrões internacionais de liberdade de expressão já atendem à questão. Eles destacam que a simples criminalização de informações consideradas falsas pode ser conflitante com esses padrões, ao conceder poder discricionário excessivo às autoridades para determinar o que seja verdade (DSN, 2022).

Enfatizando a importância da transparência e mecanismos de controle robustos, o grupo entende que é necessário fortalecer o sistema de governança, participação e transparência nas

instituições estatais para combater as campanhas de desinformação. Como medidas, propõe a criação de comitês independentes formados por especialistas da sociedade civil, setores relevantes, acadêmicos e, em alguns casos, membros do poder judicial ou autoridades independentes. Também consideram fundamental a participação de atores externos na governança para garantir a efetividade das ações. Eles ressaltam que o sigilo deve ser protegido por lei quando necessário, mas não deve ser usado como empecilho para evitar a participação da sociedade civil (DSN, 2022).

6.1.3 Iniciativas da Unesco

Em novembro de 2023, a Unesco *(United Nations Educational, Scientific and Cultural Organization)* anunciou um plano de ação para combater a desinformação e o discurso de ódio nas redes sociais. A iniciativa é consequência de um amplo processo multisetorial de consulta global realizado extensivamente em 134 países durante 18 meses. Os resultados provenientes de mais de 10 mil contribuições destacaram a urgência de adotar medidas imediatas contra as ameaças presentes no ambiente online, principalmente por entender que a digitalização da sociedade está se tornando cada vez mais predominante na sociedade mundial. Estimativas da entidade, de 2023, indicam que aproximadamente 60% da população global estiveram ativamente engajados em plataformas de redes sociais. Isso significa que 4,75 bilhões de pessoas estiveram conectadas em um ecossistema digital global para se comunicar, buscar informações e expressar suas identidades (Unesco, 2023).

O documento apresenta sete princípios fundamentais para a governança digital. Além disso, ele detalha medidas que todos os envolvidos, incluindo governos, entidades reguladoras, organizações da sociedade civil e as próprias plataformas digitais, devem ser adotar para que os resultados estejam de acordo com os propósitos estabelecidos:

> O objetivo das Diretrizes é salvaguardar o direito à liberdade de expressão, incluindo o acesso à informação e outros direitos humanos na governança de plataformas digitais, ao mesmo tempo em que tratam de conteúdo que pode ser permissivamente restringido de acordo com o direito e as normas internacionais de direitos humanos (Unesco, 2023, p. 10, tradução nossa)[37].

[37] *"The aim of the Guidelines is to safeguard the right to freedom of expression, including access to information and other human rights in digital platform governance, while dealing with content that can be permissibly restricted under international human rights law and standards".*

Esses princípios definem que as plataformas devem ter processos para avaliar continuamente os possíveis impactos de suas atividades nos direitos humanos, além de identificar possíveis riscos a esses fundamentos. A recomendação é de que essas avaliações sejam realizadas preventivamente e de forma periódica. Além disso, as revisões devem ter uma abordagem inclusiva e participativa, e contar com a contribuição de diversas partes interessadas, como usuários, grupos da sociedade civil, pesquisadores e especialistas em direitos humanos. Dessa forma, a entidade procura garantir que o ambiente online esteja alinhado com as boas práticas de transparência de suas ações perante os usuários (Unesco, 2023).

A Unesco orienta, ainda, que as plataformas digitais devem implementar ações específicas para prevenir ou reduzir os impactos adversos aos direitos humanos que forem identificados. Essas medidas podem incluir ajustes nas políticas de moderação de conteúdo, melhorias nos sistemas de denúncias, investimentos em capacitação de equipes responsáveis pela moderação, entre outras iniciativas direcionadas para mitigar os efeitos prejudiciais. Tanto os processos de avaliação quanto seus resultados devem ser transparentes e públicos, para promover a prestação de contas das plataformas (Unesco, 2023).

As diretrizes também estabelecem que as plataformas devem disponibilizar informações para os usuários, notificá-los quando os conteúdos forem removidos e permitir contestação sobre essa ação. Além disso, anúncios políticos devem ter transparência e arquivados em um registro público. Outro ponto definido é que as plataformas devem adotar medidas específicas para garantir a integridade dos processos eleitorais, como avaliações de risco eleitoral, sinalização clara de conteúdos e maior transparência da publicidade política. A Unesco ressaltou, ainda, a necessidade de proteção da liberdade de expressão, argumentando que restringir ou limitar o discurso seria altamente prejudicial. A entidade defende que a disponibilidade de meios de comunicação e ferramentas de informação independentes, de qualidade e gratuitos é a abordagem mais eficaz para combater a desinformação a longo prazo (Unesco, 2023).

Em 2015, a Conferência Geral da Unesco havia aprovado os Princípios ROAM de Universalidade da Internet *(um acrônimo para Rights, Openness, Accessibility, Multistakeholder)* com o propósito de promover o uso inclusivo, ético e transparente da internet em todo o mundo. Esses princípios estabelecem um ambiente virtual fundamentado nos Direitos Humanos e liberdades fundamentais, que promova a abertura para a livre circulação de informações e ideias e garanta a acessibilidade a todos, independentemente de diferenças socioeconômicas (Unesco, 2023).

A implementação desses princípios exige um compromisso conjunto das partes interessadas. Através da colaboração e da ação coletiva, a Unesco entende que é possível construir um futuro digital mais justo, inclusivo e respeitoso dos direitos humanos, onde as redes sociais sirvam como ferramentas para o bem, promovendo o diálogo, a informação de qualidade e a participação cidadã. Esse posicionamento tem sido constante no sistema da Organização das Nações Unidas (ONU). Desde a Cúpula Mundial sobre a Sociedade da Informação em 2003 e 2005, a estratégia global adotada pela entidade tem seguido uma abordagem multissetorial para desenvolver e aplicar princípios, normas, regras, procedimentos de tomada de decisões e programas compartilhados que influenciam a evolução e o uso da internet. Esta abordagem foi reafirmada pela Assembleia Geral das Nações Unidas durante o processo de revisão de 10 anos em 2015 (Unesco, 2023).

As diretrizes também complementam a Declaração Mondiacult de 2022, que enfatiza a necessidade de uma regulamentação do setor digital, especialmente das principais plataformas. Com isso, os delegados procuraram promover a diversidade cultural online e garantir um acesso mais igual para todos. A estratégia inclui a promoção de conteúdos diversos e culturalmente relevantes, o combate à disseminação de informações prejudiciais ou discriminatórias, e a garantia de que o acesso às plataformas seja acessível e justo para todos os usuários (Unesco, 2023).

6.1.4 Iniciativas do G7

Durante a presidência rotativa no G7[38] em 2018, o Canadá lançou uma iniciativa para fortalecer os compromissos dos líderes do fórum com a democracia e promover a proteção dos Estados-membro por meio da identificação, prevenção e resposta às ameaças estrangeiras: “Essas ameaças incluem atividades estatais hostis que visam nossas instituições e processos democráticos, nossos meios de comunicação e ambiente de informação e o exercício dos direitos humanos e das liberdades fundamentais”. Esta iniciativa foi apresentada na Cimeira Charlevoix, em junho do referido ano, e ficou conhecida como o Mecanismo de Resposta Rápida (MRR) (G7, 2022).

[38] O G7 é um fórum que reúne os sete países mais desenvolvidos e industrializados do mundo (Canadá, Estados Unidos, Reino Unido, França, Itália, Alemanha e Japão). Este grupo discute, anualmente, temas realiza de grande importância para a comunidade internacional na Cúpula do G7. Além dos sete membros oficiais, a União Europeia também participa do G7 como membro não numerado, e outros países são convidados a integrar as reuniões do grupo. O Brasil já participou de sete cúpulas do G7 nessa condição, sendo a mais recente realizada em Hiroshima, no Japão, em 2023 (Henrique, 2023).

O MRR foi concebido como um instrumento ágil e eficiente para identificar, prevenir e responder prontamente a ameaças à democracia e à estabilidade dos países do G7. Funciona como um sistema de alerta e resposta para o Canadá e seus parceiros do grupo. As funções do mecanismo são o compartilhamento de informações, análises de ameaças e identificação de oportunidades para respostas coordenadas aos desafios emergentes. Essa estrutura organizacional visa fortalecer a capacidade de antecipar, identificar e responder de forma conjunta as ameaças à segurança e estabilidade democrática. Seu objetivo é garantir uma resposta coordenada e rápida diante de situações que podem colocar em risco os valores democráticos e as instituições dos Estados-membro. Essas ameaças incluem, por exemplo, interferências em processos eleitorais, ataques cibernéticos contra infraestruturas críticas, desinformação em larga escala e outras formas de ameaças à soberania e integridade dos países integrantes (G7, 2022).

Com o sistema, foi possível identificar que as táticas de manipulação de informações usadas por atores estatais estrangeiros se tornaram mais abrangentes e sofisticadas. A tendência é de que esse fenômeno cresça a cada dia. Como exemplo de atores identificados, o G7 (2022) destaca a Rússia. O grupo assinalou que os russos ampliaram sua influência manipulando informações através de sites "clonados" de mídias internacionalmente reconhecidas, além de apoiar o crescimento de uma "indústria de desinformação" comercial. Ela direcionou sua manipulação para grupos específicos minoritários em países como Itália, Tunísia, Hungria e o Brasil, inclusive (G7, 2022).

Para fortalecer ainda mais sua eficácia e abrangência, o MRR buscou envolver parceiros externos, organizações internacionais e sociedade civil. A iniciativa foi vista como uma resposta proativa e necessária para enfrentar os desafios emergentes que ameaçam a democracia e a estabilidade global. Além disso, demonstram o compromisso do Canadá e dos demais países do G7 com os valores democráticos fundamentais e a proteção de suas instituições (G7, 2022).

O grupo identificou oito tendências significativas em 2022 relacionadas à desinformação, especificamente com participação da Rússia e da China. Primeiramente, percebeu a persistente manipulação de informações russas direcionada à Ucrânia como parte de sua estratégia para justificar a agressão territorial. Além disso, as narrativas de desinformação da Rússia evoluíram no decorrer do conflito, abrangendo temas como a "nazificação" e derrota militar da Ucrânia. A Rússia também interferiu no ambiente de informações de países africanos, incluindo Mali, Burkina Faso, Madagascar e Sudão (G7, 2022).

Também foi observado o uso crescente de redes de amplificação chinesas para a promoção de narrativas antiocidentais e que justificavam as ações da China em diferentes países. Um aumento no uso de conteúdo gerado por inteligência artificial foi outra tendência identificada neste ambiente informacional. Esse fato acrescenta sofisticação às campanhas de desinformação, ilustrando a complexidade e o problema contínuo de combater a manipulação da informação. As redes sociais foram o campo de batalha para essas atividades, tendo sido amplamente realizadas por meio desses canais, tornando-se a principal plataforma usada para espalhar conteúdo manipulado (G7, 2022).

O monitoramento realizado pelo MRR identificou uma estratégia de manipulação e interferência de informações por parte de Estados estrangeiros, que se tornou um vetor de ameaça às eleições em todo o mundo. As campanhas eleitorais, apesar de não serem o único foco dos observadores, frequentemente se tornam alvos de atividades estatais hostis. Tais ações, com motivações variadas, podem buscar influenciar o resultado das eleições, minar a confiança nas instituições democráticas ou até mesmo intensificar a polarização social (G7, 2022).

6.1.5 Iniciativas do Sudeste Asiático

No Sudeste Asiático, iniciativas intergovernamentais têm sido promovidas para combater a desinformação e proteger os direitos humanos na região. A Associação das Nações do Sudeste Asiático (ASEAN)[39] vem trabalhando no fortalecimento da cooperação regional e internacional nessa área, incluindo a da segurança e economia, para o enfrentamento de desafios como a desinformação. A associação também tem se esforçado para consolidar laços políticos e institucionais, desenvolvendo uma arquitetura normativa mais complexa para lidar com os desafios regionais e multilaterais (Asean, 2024).

Em janeiro de 2024, a Comissão Intergovernamental de Direitos Humanos da ASEAN (AICHR) realizou uma cúpula sobre desinformação e misinformação. O evento, ocorrido em Singapura, reuniu mais de 50 partes interessadas em discutir os desafios e explorar soluções para combater essas ameaças existentes contra os países da região. O grupo incluiu membros

39 A Associação das Nações do Sudeste Asiático (Asean) é uma organização intergovernamental regional que compreende dez países do sudeste asiático. Ela promove a cooperação intergovernamental e facilita a integração econômica, política, de segurança, militar, educacional e sociocultural entre seus membros e outros países. A ASEAN foi criada em 8 de agosto de 1967 por meio de um acordo entre Cingapura, Indonésia, Filipinas, Malásia e Tailândia. Além desses, atualmente fazem parte da associação: Brunei Darussalam, Camboja, Laos, Mianmar e Vietnã (Asean, S.d).

da AICHR, UE, ASEAN, organizações da sociedade civil, do setor privado, academia, meios de comunicação e investigadores políticos (Asean, 2024).

Os participantes da reunião sugeriram diversas estratégias contra a disseminação de informações falsas. Eles dividiram essas iniciativas em dois grupos principais. No primeiro, destacaram o combate à desinformação por meio da intensificação da cooperação intergovernamental, facilitando a troca de informações e melhores práticas entre os países, além de compartilhar dados, ferramentas e recursos para identificar e remover desinformação online. Também enfatizaram a importância do fortalecimento da capacidade nacional de combate a essas ameaças com o treinamento de funcionários públicos, desenvolvimento de leis e políticas relevantes, além da conscientização do público sobre os perigos da desinformação. Outro ponto destacado foi a promoção da educação midiática, implementando programas educacionais para ensinar as pessoas a identificar e verificar a veracidade das informações online (Asean, 2024).

O segundo conjunto de medidas focou no combate à desinformação referente à proteção dos direitos humanos. Isso incluiu questões como o enfrentamento às violações desses direitos, às incitações à violência, à discriminação, entre outras. Paralelamente, a proteção à liberdade de expressão foi outro ponto destacado, visando assegurar sua prática. Adicionalmente, os participantes defenderam o envolvimento da sociedade civil, enfatizando a aderência aos direitos humanos fundamentais e à integridade, fortalecendo, assim, as garantias desses direitos frente às consequências da manipulação de informações (Asean, 2024).

Sobre o impacto nos direitos humanos, Stoinski e Dias (2023) explicam que as informações falsas afetam diretamente essas questões, pois agem na autodeterminação do indivíduo. Isto porque, quando alguém é exposto a notícias manipuladas, pode perceber a realidade de maneira distorcida, afetando sua capacidade de tomar decisões baseadas em fatos. Essa prática é vista como uma violação da sua dignidade como ser humano.

6.1.6 OEA e a liberdade de expressão

Um importante documento que estabelece diretrizes para garantir a liberdade de expressão e o acesso à informação no mundo digital é a Declaração Conjunta sobre Desafios para a Liberdade de Expressão na Próxima Década (JCDCLEPD, na sigla em inglês). Assinada em 2019 pela Organização dos Estados Americanos (OEA), Organização para a Segurança e Cooperação na Europa (OSCE), ONU e Comissão Africana, a declaração enfatiza o reconhecimento desses direitos como fundamentais para a democracia e a participação cidadã. O documento prevê a regulamentação e a supervisão das companhias de comunicação digital

como medidas necessárias para evitar a concentração do mercado de comunicação digital por um pequeno grupo de empresas.

As entidades reconhecem a importância crescente dessas plataformas como espaços para que os cidadãos possam se expressar e interagir socialmente, defendendo o acesso livre à informação nesses ambientes digitais. Outro ponto destacado é a garantia da transparência, da responsabilidade e da não discriminação no fornecimento dos serviços. Além disso, estabelece princípios e diretrizes para promover a concorrência justa, a pluralidade de opiniões e a proteção dos direitos humanos no contexto digital. Essas medidas visam a promoção de um ambiente mais equitativo e diversificado para o exercício da liberdade de expressão (OEA, 2019).

O documento ainda prevê a criação de mecanismos para avaliação das regras de moderação de conteúdo, que sejam imparciais, transparentes e multisetoriais. A participação de representantes da sociedade civil, academia e especialistas em direitos humanos é destacada como sendo fundamental nesse processo. Além disso, ressalta a necessidade de que essas regras moderadoras estejam em conformidade com o direito internacional dos direitos humanos e não interfiram indevidamente no exercício da liberdade de expressão dos indivíduos (OEA, 2019).

Outra preocupação crescente, que favorece a disseminação de desinformação e conteúdos prejudiciais online, são os modelos de negócios baseados em publicidade. Para coibir o abuso dessas plataformas, que visam retorno econômico com a criação de ambientes que facilitem a viralização da desinformação, discursos de ódio e outros conteúdos prejudiciais, as entidades propõem a adoção de medidas regulatórias que estabeleçam padrões de conduta e responsabilizem as plataformas por suas ações. Ao definir diretrizes claras, promover a responsabilidade, supervisionar e fiscalizar as atividades das plataformas, e exigir transparência e prestação de contas *(accountability),* as regulamentações promovem o desenvolvimento de soluções para lidar com os desafios emergentes no cenário digital (OEA, 2019).

Adicionalmente, as entidades indicam os Princípios Orientadores da ONU sobre Empresas e Direitos Humanos[40] como referência para essas empresas, fornecendo um arcabouço ético e legal para orientar suas políticas e práticas. Esses princípios ajudam a garantir que as plataformas digitais operem de maneira consistente com os padrões internacionais de direitos humanos. O respeito a esses direitos em todas as atividades empresariais, é incentivado por meio da adoção de medidas que visam prevenir violações e remediar os impactos adversos que possam surgir (OEA, 2019).

[40] Esses princípios visam orientar as empresas a adotarem um padrão global de conduta em relação aos direitos humanos, promovendo a responsabilidade corporativa e o respeito aos direitos fundamentais estabelecidos internacionalmente (ONU, 2019).

Além de incentivar a proatividade das empresas, o documento enfatiza a importância de os governos implementarem regulamentações ou mecanismos de supervisão nacionais. Esse arcabouço legal é fundamental para garantir que as organizações minimizem os danos aos direitos humanos resultantes das atividades online. Concomitantemente, o estabelecimento de compromissos públicos, políticas e avaliações de impacto sobre seus efeitos nos direitos do indivíduo por essas plataformas é um caminho importante para a correção de quaisquer violações ou efeitos adversos (OEA, 2019).

A Declaração prevê, ainda, a possibilidade de soluções tecnológicas na moderação do conteúdo online, como os algoritmos de inteligência artificial. Seu uso é aceito desde que haja transparência e que as moderações sejam compreensíveis e justificáveis. Esses algoritmos podem identificar e remover conteúdo prejudicial de forma automática, como discurso de ódio, desinformação e conteúdo violento. Entretanto, as regras de funcionamento e decisões desses algoritmos precisam ser claras e acessíveis ao público (OEA, 2019).

Por fim, as instituições defendem que a concentração de propriedade e abuso de poder no mercado de comunicação digital deva ser combatida para garantir um ambiente mais justo, democrático e plural. Para isso, é importante estabelecer regulamentos e sistemas eficazes para abordar a concentração indevida de propriedade e práticas abusivas de poder no (OEA, 2019).

6.2 INICIATIVAS DO BRASIL

Em um esforço para combater a desinformação e defender a integridade da informação, as principais agências de fomento e pesquisa do Brasil se uniram por meio de uma parceria estratégica. A rede, composta pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), Financiadora de Estudos e Projetos (FINEP), Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT) e Instituto de Pesquisa Econômica Aplicada (Ipea), foi estabelecida para fortalecer a pesquisa e a colaboração entre os setores público e acadêmico a fim de enfrentar esse desafio emergente. Além de compreender os mecanismos de propagação de notícias falsas, a proposta busca elaborar e implementar estratégias eficazes para diminuir seu impacto negativo (G20, 2024).

O grupo definiu um protocolo de intenções para apoiar projetos que combatam a desinformação e os discursos de ódio. Com o objetivo de criar uma abordagem multidisciplinar e abrangente, o consórcio estabeleceu a formação de uma rede de pesquisa científica e de um fórum de parcerias. Para organizar e dar suporte aos projetos, está previsto o desenvolvimento

de uma plataforma de dados que centralizará a coleta, análise e compartilhamento de informações relevantes, permitindo uma troca contínua de conhecimento e melhores práticas. Além de promover a pesquisa e o desenvolvimento de tecnologias e metodologias para combater esses problemas, o consórcio incentiva a construção de políticas públicas para criar um ambiente mais propício à mitigação desses fenômenos (G20, 2024).

Outra iniciativa brasileira partiu do Tribunal Superior Eleitoral (TSE). O órgão lançou, em 2019, o Programa de Enfrentamento à Desinformação (PED), com o objetivo de identificar os principais desafios decorrentes da disseminação da desinformação. O projeto propõe a criação de soluções eficazes que fortaleçam a integridade do sistema eleitoral, garantindo, assim, a legitimidade e a transparência das eleições. A iniciativa conta com mais de 150 parceiros, como plataformas digitais, redes sociais, entidades profissionais e instituições públicas e privadas, entre outros. O programa se tornou uma ação perene em 2021, passando a se chamar Programa Permanente de Enfrentamento à Desinformação (PEED), com foco nas eleições de 2022 (TRE, 2023).

No plano de ação do PEED, foram estabelecidos três eixos que adotam medidas a serem realizadas no curto, médio e longo prazo. O primeiro eixo “informar” adota a informação como uma ferramenta para lidar com a desinformação. O objetivo é permitir que os cidadãos formem suas convicções de maneira consciente, baseadas em fatos e em uma compreensão clara da situação, em oposição a crenças ou opiniões distorcidas pela desinformação (TSE, 2023).

O segundo eixo “capacitar” tem como objetivo principal treinar tanto o cidadão quanto os servidores da Justiça Federal para desenvolverem competências e conhecimentos essenciais a fim de identificar e lidar com a propagação de informações falsas e enganosas. O terceiro eixo “controlar” visa enfrentar a desinformação monitorando comportamentos inautênticos e ações coordenadas que disseminam desinformação, utilizando dados abertos das redes sociais e recursos tecnológicos (TSE, 2023).

Complementando o PEED, foi criado o Programa de Fortalecimento Institucional (PROFI), com o propósito de implementar ações que visam melhorar a imagem das instituições eleitorais, promovendo uma percepção mais positiva em relação à imparcialidade, profissionalismo e importância da Justiça Eleitoral. Os projetos se estruturam em dois eixos interligados, que estão relacionados à gestão de riscos de reputação (eixo preventivo) e à construção de uma imagem sólida e favorável do setor judiciário eleitoral (eixo afirmativo) (TSE, 2023).

Além dessas iniciativas, o TSE realizou diversas ações para combater a desinformação e fortalecer a credibilidade das instituições eleitorais durante as Eleições de 2022. Dentre essas,

destacam-se a criação da Assessoria Especial de Enfrentamento à Desinformação (AEED); a implementação do Sistema de Alerta de Desinformação Contra as Eleições; o aprimoramento de um *chatbot* em parceria com o WhatsApp, que atingiu mais de 6,2 milhões de usuários ativos; e a criação de um canal oficial no Telegram com quase 375 mil usuários. Além disso, foi idealizada uma central de notificações por meio de aplicativos da Justiça Eleitoral, abrangendo cerca de 40 milhões de usuários (TSE, 2023).

O tribunal também ampliou a rede de difusores de conteúdos de qualidade sobre as instituições eleitorais; e lançou uma página online denominada "Fato ou Boato" em conjunto com uma rede de empresas privadas de checagem de fatos. Outras medidas adotadas foram a ampliação da rede de monitoramento de dados abertos em redes sociais; a contratação de serviço de monitoramento digital de narrativas falsas; a instituição da "Frente Nacional de Enfrentamento à Desinformação" com mais de 2,1 mil voluntários; e o desenvolvimento de ferramenta de *Business Intelligence* para acompanhamento de eventos e atividades (TSE, 2023).

Outra iniciativa partiu do governo federal que, em março de 2023, lançou o portal "Brasil contra Fake" para combater a desinformação relacionada às ações institucionais e às políticas públicas que são alvo de distorções. O site funciona como um provedor de informações oficiais para as instituições públicas e também para a população, combatendo as notícias falsas que possam prejudicar a sociedade e a democracia (Brasil, 2023a).

O lançamento do portal contou com uma campanha publicitária, com o tema "Quem espalha *'fake News'* espalha destruição". Os objetivos da campanha foram sensibilizar a sociedade sobre os perigos das notícias falsas e da desinformação, e comunicar os esforços governamentais no combate à produção e disseminação dessas notícias. A atividade promocional também procurou engajar a sociedade no combate às *fake news* e orientar a população sobre os procedimentos que devem ser adotados para identificar e verificar a veracidade de informações suspeitas (Brasil, 2023a).

Ainda que não se configure essencialmente como uma agência de verificação de fatos, o portal é concebido como um espaço governamental voltado para esclarecimentos. Contudo, alguns especialistas se preocupam com a transparência e imparcialidade dessa iniciativa, característica fundamental para garantir a eficácia de projetos de checagem de fatos (*fact-checking*). De acordo com Seibt (2023), além da necessidade de apresentar esses elementos, é necessário que as práticas adotadas em todo o processo sejam rigorosas e garantam a precisão e a confiabilidade das informações divulgadas. Ela explica que, segundo o código de princípios da *International Fact-Checking Network (IFCN),* o apartidarismo é um princípio fundamental na atividade de verificação de fatos. Isso significa que uma iniciativa governamental não pode

ser credenciada pela instituição, pois não atende a esse requisito. No entanto, segundo a autora, isso não impede que o governo adote o formato de *fact-checking*, desde que siga critérios transparentes, evite a autorreferência e se comprometa com a verdade factual.

Ainda com base nesse entendimento, Tardáguila (2023) ressalta que o uso de uma única fonte para refutar as informações falsas, indica que o "Brasil contra Fake" restringe o acesso a conteúdos abrangentes, variados e isentos de viés político:

> Dados produzidos por governos são importantes em muitos casos em que a veracidade de um conteúdo está em disputa. Mas, no trabalho de checagem profissional, eles não devem nem podem ser tomados como fonte absoluta – menos ainda se o tema estiver relacionado a eles. Além disso, a indicação do próprio Executivo como fonte única e exclusiva para desmentidos, como faz o "Brasil contra fake", sinaliza um movimento interno e cíclico de apuração, que limita o acesso do cidadão a informações mais amplas, diversas e apartidárias sobre os assuntos abordados pelo programa (Tardáguila, 2023, s.p.).

No direito ao contraditório, a Secretaria de Comunicação (Secom) da Presidência da República do Brasil, argumenta, segundo o autor, que os textos divulgados na plataforma são informações oficiais, compiladas e publicadas em canais como o Diário Oficial da União, legislações aprovadas pelo Congresso Nacional, decretos presidenciais e comunicados ministeriais. Dessa forma, essas informações possuem amparo jurídico e fazem parte integrante das políticas públicas implementadas pelo Poder Executivo Federal. A fundamentação jurídica e a origem oficial dessas informações lhes conferem legitimidade e confiabilidade, constituindo-se em um contraponto importante às notícias falsas que possam circular na sociedade.

O Ministério da Justiça e Segurança Pública do Brasil também tem adotado algumas iniciativas relevantes no combate à desinformação. A Secretaria de Direitos Digitais (SEDIGI) lançou o site "De Boa na Rede" voltado para campanhas de proteção dos direitos dos cidadãos no ambiente digital. O objetivo é promover um espaço virtual seguro para crianças e adolescentes, promovendo a conscientização da população sobre os riscos da desinformação. O site conta com ferramentas de controle parental para redes sociais, jogos digitais e *streaming*, além de dicas e tutoriais para as famílias sobre como monitorar o conteúdo acessado pelos jovens. Também traz informações sobre tipos de crimes praticados na internet e como denunciá-los (Brasil, 2023b). Além disso, a Autoridade Nacional de Proteção de Dados (ANPD), vinculada ao ministério, vem desempenhando um importante papel na regulação e fiscalização do uso de dados pessoais, o que

pode contribuir indiretamente para coibir o uso indevido de informações para a disseminação de conteúdo enganoso.

Outra frente de atuação foi promovida pela Diretoria de Ensino e Pesquisa (DEP) da Secretaria Nacional de Segurança Pública (Senasp/MJSP). O órgão incentiva o fortalecimento da democracia por meio da capacitação de agentes públicos. Em conjunto com a Secretaria Nacional de Direitos Digitais, os servidores são treinados para o enfrentamento da desinformação, a fim de garantir um ambiente digital seguro para toda a sociedade, especialmente em relação às atividades eleitorais (Brasil, 2024).

Cabe também destacar o Projeto de Lei das *fake news*, conhecido como PL 2630/2020, de autoria do Poder Legislativo brasileiro, que visa instituir a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. O objetivo dessa proposta é a criação de normas de transparência nas redes sociais e serviços de mensagens privadas, em especial no que diz respeito à responsabilidade dos provedores no que se refere à desinformação. O projeto exige ainda que as plataformas compartilhem informações sobre os algoritmos que são usados para direcionar o conteúdo para os usuários e criem mecanismos para exclusão e notificação de conteúdos ilegais e prejudiciais (Brasil, 2020b).

O PL das *fake news* sugere várias ações, como a proibição de contas, perfis ou robôs falsos e não identificados, a criação de um conselho de transparência e responsabilidade, a rotulagem e limitação de alcance do conteúdo enganoso, e a exclusão ou suspensão de contas que violem os termos de uso ou legislação vigente. Este projeto tem gerado bastante controvérsia e discussão na esfera social. Por um lado, seus defensores indicam sua importância e necessidade para a democracia e os direitos humanos, por outro, os críticos levantam possíveis implicações na censura e violações à privacidade dos indivíduos (Xavier, 2024).

O Supremo Tribunal Federal (STF) também tem se posicionado contra essas ameaças. Em 2021, a entidade lançou o Programa de Combate à Desinformação (PCD), visando combater práticas como *fake news* e discursos de ódio que afetam a confiança pública no tribunal, distorcem ou alteram o significado de suas decisões, e ameaçam direitos fundamentais e a estabilidade democrática. Por meio do programa, são desenvolvidos projetos, ações e produtos em parceria com diversas entidades, incluindo universidades, Organizações Não Governamentais (ONGs) e institutos de checagem de informações enganosas. As ações incluem alfabetização midiática de servidores, funcionários terceirizados, jornalistas e influenciadores digitais para capacitação contra a desinformação; contestação de notícias falsas por meio da série "#VerdadesdoSTF"; publicada no site e nas redes sociais da instituição, além da valorização de conteúdos que geram engajamento positivo (Supremo Tribunal Federal, 2021).

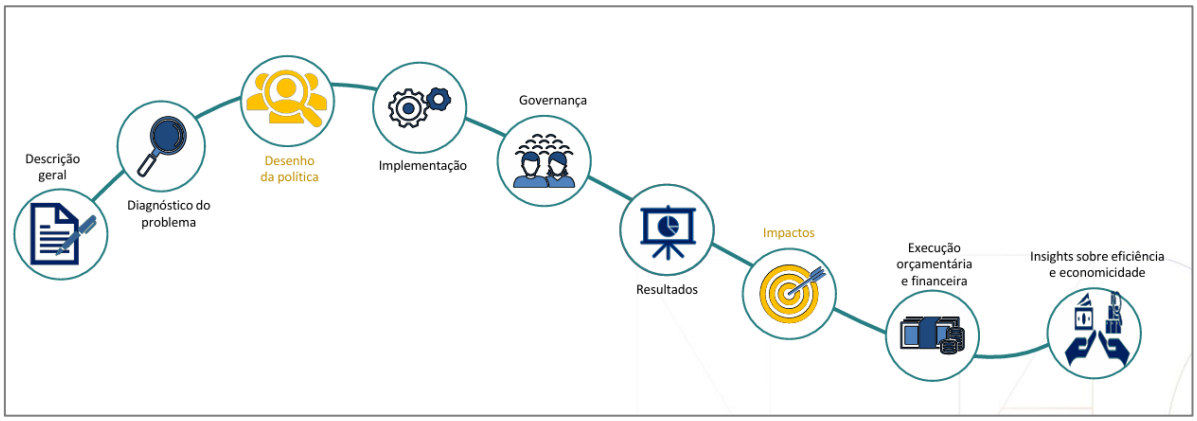
6.2.1 Evolução das políticas públicas brasileiras de defesa nacional

Pilar fundamental da segurança e da soberania do país, a defesa nacional é estabelecida por meio de políticas públicas destinadas a manter a integridade territorial e os interesses nacionais do país contra ameaças internas e externas. Promulgadas por meio de decretos e portarias, as políticas públicas de defesa nacional assumem um papel determinante para a salvaguarda da soberania nacional e proteção do patrimônio e dos interesses do país. Esse arcabouço legal possui fundamental importância para a consolidação das instituições e do Estado Democrático de Direito, além de promover a projeção do Brasil no cenário internacional, ampliando sua influência no processo decisório global (Ipea, 2023a).

Com a finalidade de dar conhecimento à sociedade, promover a transparência e sistematizar o conjunto de políticas públicas instituídas pelo Poder Executivo Federal, o Instituto de Políticas Econômicas Aplicadas (Ipea, 2023b) disponibilizou em uma plataforma virtual um catálogo com mais de 660 iniciativas. O site é uma fonte de dados para estudos e análises que auxiliam no entendimento das proposições e do funcionamento dessas normativas. As políticas abrangem um amplo espectro de público-alvo, com temáticas que englobam desde a segurança da população em geral e a preservação do meio ambiente até o Sistema de Pesquisa Espacial e o Sistema Nacional de Defesa (Ipea, 2023a).

Destaca-se que a promoção e eficácia desses programas governamentais são realizadas pelo Conselho de Monitoramento e Avaliação de Políticas Públicas (CMAP) composto por secretários executivos de cinco ministérios, a partir de programas finalísticos do Plano Plurianual (PPA). As ações da CMAP são acompanhas tecnicamente pelo Comitê de Monitoramento e Avaliação de Gastos Diretos (CMAG) e do Comitê de Monitoramento e Avaliação dos Subsídios da União (CMAS), que compõem a estrutura. Esses colegiados têm como função principal elaborar critérios de seleção de políticas públicas a serem avaliadas, acompanhar a implementação dessas iniciativas e propor aprimoramentos com base nos resultados das avaliações. Eles também são responsáveis por solicitar informações aos órgãos gestores, consolidar essas informações e garantir a transparência de seus atos (Brasil, 2023e). O ciclo de avaliação é um processo de elaboração colaborativa que recebe aprimoramentos constantes. A série de 2023 contemplou nove etapas, conforme a Figura 3 a seguir:

Figura 3 - Ciclo 2023 de avaliação das políticas públicas



Fonte: Santos (2023).

6.2.2 Panorama histórico

O catálogo geral do Ipea (2023a) agrega 25 políticas públicas na área de Defesa Nacional com base em um ordenamento histórico. A primeira política enquadrada nesta temática foi promulgada por meio do Decreto nº 98.498, em 12 de dezembro de 1989. O documento se refere à aprovação e execução do Programa Desportivo Militar Anual das Forças Armadas (PDMAF), para o ano de 1990. As outras iniciativas abordam temas como Defesa Nacional, Segurança Pública, Ciência, Tecnologia e Inovação, Espacial, Recursos do Mar, Defesa e Segurança Marítima, Esporte, Segurança da Informação e Cibernética e Inteligência, conforme organizado na tabela a seguir. A proposta da plataforma é realizar uma atualização permanente do inventário devido às dinâmicas do Estado brasileiro.

Tabela 2. Listagem do catálogo do Ipea sobre políticas públicas da área de Defesa

Ano	Documento	Tema Principal
1989	Programa Desportivo Militar Anual das Forças Armadas	Esporte
1994	Política Nacional de Desenvolvimento das Atividades Espaciais	Espacial
1996	Política de Defesa Nacional	Defesa Nacional
2005	Política Nacional da Indústria da Defesa	Defesa e Segurança Marítima
2005	Política Nacional para os Recursos do Mar (PNRM)	Recursos do Mar
2008	Estratégia Nacional de Defesa	Defesa Nacional
2010	Política de Ensino de Defesa	Defesa Nacional
2010	Política de Mobilização Nacional	Defesa Nacional

Ano	Documento	Tema Principal
2012	Plano de Articulação e Equipamento da Defesa	Defesa Nacional
2016	Política Nacional de Inteligência	Defesa Nacional
2016	Programa de Proteção Integrada de Fronteiras	Segurança Pública
2018	Política Nacional de Defesa	Defesa Nacional
2018	Política Nacional de Exportação e Importação de Produtos de Defesa	Defesa Nacional
2021	Política Nacional de Ciência, Tecnologia e Inovação de Defesa	Ciência, Tecnologia e Inovação
2021	Política Nacional de Inteligência de Segurança Pública	Segurança Pública
2021	Plano Nacional de Segurança Pública e Defesa Social 2021-2030	Segurança Pública
2021	Política de Educação Física e Desportos da Marinha do Brasil	Esporte
2021	Programa Nacional de Segurança nas Fronteiras e Divisas - VIGIA	Segurança Pública
2022	Política Nacional da Base Industrial de Defesa - PNBID	Defesa Nacional
2022	Política Nacional para Assuntos Antárticos	Defesa Nacional
2022	Política de Segurança da Informação da administração central do Ministério da Defesa - POSIN-MD	Defesa Nacional
2023	Plano Estratégico Setorial 2024-2027	Defesa Nacional
2023	Política Nacional de Cibersegurança	Defesa Nacional
2023	Plano Setorial de Gestão de Incidentes Cibernéticos do Setor Defesa (PSGIC-Def)	Defesa Nacional
2023	Política de Inteligência de Defesa	Defesa Nacional

Fonte: Elaborado pela autora com base em Ipea (2023a).

Considerando a relevância das políticas citadas para o atendimento dos objetivos desta pesquisa, foram selecionadas as iniciativas a seguir. Ao término desta análise contextualizada, serão discutidas as possíveis sinergias regulatórias como base para políticas públicas no contexto do Ministério da Defesa.

6.2.3 Política Nacional de Defesa e Estratégia de Defesa Nacional

A Política Nacional de Defesa (PND) é o documento de maior hierarquia para nortear o planejamento de ações voltadas à defesa do país, fundamentada na análise dos contextos nacional e internacional vigentes (Câmara dos Deputados, 2024). Instituída originalmente em 1996 como Política de Defesa Nacional (PDN) (Brasil, 1996), a normativa passou a se chamar Política Nacional de Defesa em 2012, a partir de revisões quadrienais. Uma nova edição foi

publicada em 2020, e a versão mais recente foi enviada ao Senado e depois à Câmara dos Deputados, tendo sido aprovada em 15 de maio 2024, seguindo, posteriormente, para promulgação (Brasil, 2024b).

A PND se destaca como o documento fundamental que norteia a defesa do Brasil. Nele, são definidos os objetivos, conceitos e diretrizes que garantem a soberania nacional e a proteção do patrimônio e dos interesses do país. Também estão incluídos o fortalecimento do Estado de Direito e das instituições democráticas e a projeção do Brasil no cenário internacional (Brasil, 2024b).

Mais do que um instrumento de proteção normativa para a nação, a PND é um documento condicionante que estabelece metas claras e orienta o Estado brasileiro sobre como alcançá-las, abrangendo tanto o setor militar quanto o civil. Através de uma análise profunda dos ambientes nacional e internacional, a PND define os Objetivos Nacionais de Defesa, servindo como base para a Estratégia Nacional de Defesa (END), que por sua vez detalha as diretrizes para o emprego das Forças Armadas (Brasil, 2024b).

Em conjunto, a PND e a END se configuram como fundamentos para a segurança do Brasil. O documento que apresenta de forma detalhada a política de defesa do país, as estratégias, as capacidades e a estrutura das Forças Armadas é o Livro Branco da Defesa Nacional (LBDN), elaborado pelo Ministério da Justiça. A publicação alinha as políticas de defesa com os interesses e valores da sociedade, oferecendo transparência e promovendo o entendimento das ações por parte da população e da comunidade internacional (Brasil, 2024c).

6.2.4 Política Nacional de Inteligência

A Política Nacional de Inteligência (PNI) é um documento de alto nível que define os parâmetros e limites de atuação da atividade de inteligência no Brasil. Estabelecida pelo Decreto nº 8.793, em 29 de junho de 2016, a PNI tem como objetivo fortalecer o Sistema Brasileiro de Inteligência (SISBIN), que é composto por 37 agências. Esse fortalecimento visa permitir uma integração eficiente entre essas entidades para subsidiar o Estado brasileiro na tomada de decisões estratégicas (Brasil, 2017).

A PNI, em conjunto com a Estratégia Nacional de Inteligência (ENINT), estabelece as diretrizes e orientações para a atividade de inteligência no Brasil. Elas definem como a inteligência deve ser coletada, analisada e utilizada para proteger o país e apoiar a tomada de decisões estratégicas. Seus instrumentos essenciais incluem planos, doutrina, diretivas, o SISBIN, intercâmbio de dados, capacitação de pessoal, pesquisa e desenvolvimento

tecnológico, recursos financeiros, e controle interno e externo. A coordenação das atividades de inteligência no âmbito do SISBIN é de responsabilidade do Gabinete de Segurança Institucional da Presidência da República. Assim, a PNI, como documento orientador para a atividade de inteligência no Brasil, estabelece os parâmetros e limites de atuação para fortalecer o SISBIN e apoiar o Estado na tomada de decisões estratégicas (Brasil, 2017).

6.2.5 Política Nacional de Ciência, Tecnologia e Inovação de Defesa

Aprovada pela Portaria Normativa do Ministério da Defesa em 2004, e atualizada em 2021, a Política Nacional de Ciência, Tecnologia e Inovação de Defesa (PCTID) apresenta objetivos estratégicos e orienta as instituições envolvidas em atividades de Ciência, Tecnologia e Inovação (C,T&I) de interesse da Defesa. Seu objetivo é criar um ambiente que estimule a pesquisa, aproveite o conhecimento científico, fomente o desenvolvimento industrial e gere produtos inovadores alinhados aos interesses das Forças Armadas (Brasil, 2021).

Seu propósito é promover o desenvolvimento de um complexo integrado entre o setor militar, acadêmico e empresarial, focado em tecnologias de vanguarda relevantes para a Defesa, com potencial de uso dual. Para isso, a política prevê a implementação de medidas que protejam os interesses de segurança do Estado no acesso a informações, ao mesmo tempo em que promovam parcerias entre o Governo, a Base Industrial de Defesa (BID), instituições científicas, tecnológicas e de inovação (ICTs) e universidades (Brasil, 2022).

6.2.6 Política Nacional de Inteligência de Segurança Pública e Plano Nacional de Segurança Pública e Defesa Social

A Política Nacional de Inteligência de Segurança Pública (PNISP) normatiza a atividade de inteligência no âmbito da segurança pública. Ela é concebida com base nos valores e princípios fundamentais da Constituição, alinhada com a Política Nacional de Inteligência (PNI), a Política Nacional de Segurança Pública e Desenvolvimento Social (PNSPDS) e os fundamentos doutrinários da atividade de inteligência de segurança pública (Brasil, 2021b).

Para atender aos objetivos da PNISP, foi estruturado o Plano Nacional de Segurança Pública e Defesa Social 2021-2030, um documento orientador que prevê a implementação de um sistema de governança com inclusão de mecanismos de liderança, estratégia e controle, por meio de um Comitê de Governança Estratégica. Esse comitê tem como objetivo avaliar, direcionar e monitorar a gestão e a condução da política pública de segurança, seguindo as

diretrizes estabelecidas pelo governo federal. O Plano conta com 13 metas principais e 12 ações estratégicas avaliadas anualmente pelo Ministério de Justiça e Segurança Pública. A aferição dessas metas e ações é realizada com o suporte de um Sistema Nacional de Informações – uma plataforma integrada que permite consultas operacionais, investigativas e estratégicas sobre segurança pública, inclusive no ambiente digital (Brasil, 2021c).

6.2.7 Política Nacional de Segurança da Informação da administração central do Ministério da Defesa

A Política de Segurança da Informação da administração central do Ministério da Defesa (POSIN-MD) tem um papel essencial na proteção das informações sensíveis do país. Esse documento estabelece diretrizes claras, definindo responsabilidades e competências para a gestão da segurança da informação dentro do Ministério da Defesa (MD). Seu principal objetivo é assegurar a confidencialidade, integridade e disponibilidade dos dados (Brasil 2022b).

Aprovada pela Portaria MD nº 5.659, de 28 de novembro de 2022, a POSIN-MD integra a legislação do Ministério da Defesa, junto com outras normas e portarias relacionadas à segurança da informação, e é fundamental para proteger informações críticas que podem afetar a segurança nacional. A política engloba a segurança cibernética, defesa cibernética, segurança física, como a salvaguarda de instalações, equipamentos e documentos que armazenam informações sensíveis (Brasil, 2022b).

6.2.8 Política de Inteligência de Defesa

A Política de Inteligência de Defesa (PID) delineia os parâmetros e limites de atuação da Atividade de Inteligência de Defesa (AID), e estabelece seus fundamentos, ameaças, objetivos e diretrizes dentro do Sistema de Inteligência de Defesa (SINDE). Serve como um guia para a AID e é estabelecida conforme a missão constitucional das Forças Armadas, os princípios da Política Nacional de Inteligência (PNI), os aspectos da Política Nacional de Defesa (PND) e da Estratégia Nacional de Defesa (END). Além disso, promove a produção de conhecimentos para embasar o emprego do poder militar e garantir a consciência situacional dos comandantes militares (Brasil, 2023c).

A PID demanda o constante aprimoramento das técnicas, da doutrina e dos recursos humanos das FFAA, servindo como base para o fortalecimento das estruturas do SINDE. Seus

principais objetivos são: auxiliar no processo de tomada de decisão, facilitar a coordenação das atividades das Forças e concentrar os esforços das diversas áreas militares para garantir a obtenção de informações relevantes e oportunas. Essas informações são essenciais para que as autoridades militares e civis tenham uma compreensão abrangente e atualizada do cenário em todos os níveis de decisão dentro do Sistema de Inteligência de Defesa (Brasil, 2023c).

6.2.9 Política Nacional de Cibersegurança

Instituída pelo Decreto nº 11.856, de 26 de dezembro de 2023, a Política Nacional de Cibersegurança (PNCiber) define a estratégia nacional para orientar a atividade de segurança cibernética, incluindo a proteção da infraestrutura crítica do país contra crimes virtuais e outras formas de guerra cibernética. O marco legal promove a cooperação entre governo, setor privado e sociedade civil para fortalecer a cibersegurança nacional (Brasil, 2023).

Seus princípios e objetivos incluem o desenvolvimento de mecanismos de regulação, fiscalização e controle, bem como estimular o desenvolvimento de produtos, serviços e tecnologias de origem nacional voltados para a cibersegurança. A PNCiber é um instrumento para assegurar a confidencialidade, integridade, autenticidade e disponibilidade das soluções e dados usados para processamento, armazenamento e transmissão eletrônica ou digital de informações. Além disso, procura reforçar a presença ativa e cuidadosa no ciberespaço, especialmente entre crianças, adolescentes e idosos, e promover a educação e capacitação técnico-profissional em segurança cibernética na sociedade (Brasil, 2023).

O Comitê Nacional de Cibersegurança (CNCiber), criado pelo mesmo decreto, é responsável por assessorar o presidente da República na formulação, coordenação e monitoramento da política. Composto por representantes de diversos ministérios e órgãos, a sua secretaria executiva é exercida pelo Gabinete de Segurança Institucional da Presidência (Brasil, 2023). Apesar de figurar no catálogo de políticas públicas de Defesa Nacional do Ipea, a PNCiber apresenta uma abordagem mais ampla e setorial para a cibersegurança do país de uma forma geral, estando sob a responsabilidade da Presidência da República. No âmbito do Ministério da Defesa, o documento que prioriza as necessidades específicas do Ministério específico é a Doutrina Militar de Defesa Cibernética (Brasil, 2023d).

6.2.10 Doutrina Militar de Defesa Cibernética

Anterior à Política Nacional de Cibersegurança (PNCiber), a Doutrina Militar de Defesa Cibernética (DMDC), aprovada pelo Ministério da Defesa, estabelece os fundamentos e diretrizes para a atuação das Forças Armadas na defesa do Brasil no espaço cibernético. Este documento abrange aspectos conceituais, organizacionais e operacionais, com o objetivo de estabelecer uma estrutura e facilitar a cooperação. Ele estabelece que a segurança cibernética é de competência da Presidência da República, enquanto a defesa cibernética fica sob a responsabilidade do Ministério da Defesa (Brasil, 2023d).

A doutrina também estabelece os níveis de decisão para ações no espaço cibernético (político, estratégico, operacional e tático), define conceitos fundamentais de defesa e segurança cibernéticas, e cria uma base conceitual sólida. Além disso, considera cenários de enfrentamento, os atores envolvidos, os recursos necessários e as formas de atuação diante de ameaças à segurança cibernética. O documento inclui a participação de setores não militares da sociedade, e promove a cooperação internacional dentro do Sistema Militar de Defesa Cibernética (Brasil, 2023d).

6.3 INICIATIVAS COMPLEMENTARES

6.3.1 Marco Civil da Internet

O Marco Civil da Internet (MCI), instituído em 2014, estabeleceu princípios e garantias para o uso da internet no Brasil, incluindo a neutralidade de rede – que impede a discriminação de conteúdos, serviços ou aplicações –, e a proteção da privacidade e dos dados pessoais dos usuários. Com esses objetivos, esse marco legal, estabelecido como medida de garantia do exercício da cidadania nos meios digitais, define a responsabilidade dos provedores de serviços em relação ao conteúdo gerado pelos usuários, a remoção de conteúdo ilegal ou que viole direitos de terceiros, entre outros (Brasil, 2014).

Em 2022, uma medida provisória alterou o MCI para incluir esclarecimentos sobre os direitos dos usuários de redes sociais. Essa medida inseriu dispositivos para garantir informações transparentes sobre as políticas de moderação de conteúdo, além do direito ao contraditório e à defesa ampla em casos de moderação feita pelas redes sociais. Também prevê o direito dos usuários de recuperarem o conteúdo que postaram e exige uma justificativa clara para cancelamentos ou suspensões de contas ou perfis, assim como para exclusão de conteúdo.

Além disso, ficou estabelecido que as redes sociais devem notificar os usuários sobre as medidas tomadas e fornecer informações sobre como contestar ou revisar as decisões (Brasil, 2021d).

6.3.2 Lei Geral de Proteção de Dados Pessoais

Sancionada em 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), complementou o MCI, especificando como devem ser realizados o armazenamento, coleta, tratamento e compartilhamento de informações, além de classificar os tipos de informação e incluir materiais físicos. Rocha (2014) explica que, enquanto o MCI trata da proteção de dados de forma mais ampla como um princípio, a LGPD detalha as regras sobre o tratamento de dados pessoais, estabelecendo bases legais adicionais que vão além do consentimento.

Apesar dos documentos apresentarem objetivos complementares, existem alguns conflitos devido à sobreposição de seus dispositivos legais. Um dos requisitos do MCI é que apenas o consentimento do usuário seja necessário para que a coleta, uso, armazenamento e tratamento de dados sejam realizados. A LGPD, além do consentimento, prevê outras bases legais, que inclui o tratamento dos dados de terceiros, como a permissão para execução de políticas públicas, desde que respeitados os princípios definidos para a administração pública. Além disso, prevê sanções para infrações, o que não ocorre no MCI. Para resolver esses conflitos, aplicam-se critérios jurídicos, considerando a LGPD como lei mais específica e posterior ao MCI (Rocha, 2024).

6.3.3 Projeto de Lei das fake news e Projeto de Lei da Inteligência artificial

Na agenda do Congresso, encontrava-se em tramitação, até o momento dessa pesquisa, o projeto de lei conhecido como o Projeto de Lei das *fake news* (PL 2.630/2020), cujo objetivo é tratar a questão da disseminação de notícias falsas e regulamentar as atividades das grandes empresas de tecnologia, responsáveis pelas plataformas digitais. Devido ao seu grande impacto, os desafios da desinformação, regulação da inteligência artificial e transparência das redes sociais ganham espaço nos debates da sociedade. A proposta quer responsabilizar as grandes empresas de tecnologia pela disseminação de conteúdo através de seus algoritmos (Brasil, 2014).

A regulação da inteligência artificial também está em debate com outro projeto de lei. O PL 2.338/2023 prevê a definição de fundamentos e sanções para o uso dessa tecnologia. Inspirado na legislação da União Europeia (AI Act) e em projetos anteriores, o PL destaca a importância dos direitos fundamentais, a segurança dos sistemas, a preservação do regime democrático e seu avanço científico e tecnológico (Brasil, 2023f).

Com o intuito de assegurar uma abordagem abrangente, o projeto propõe a Autoridade Nacional de Proteção de Dados (ANPD) como órgão competente para regular e governar a IA no país, a fim de evitar uma fragmentação regulatória. Além disso, estabelece medidas de governança para órgãos públicos que utilizem esses sistemas, considerados de alto risco, como a realização de consultas públicas, definição de protocolos de acesso e garantia da utilização de dados seguros (Brasil, 2023f).

6.3.4 Resoluções contra o uso da Inteligência artificial nas eleições

O Tribunal Superior Eleitoral (TSE, 2024) também implementou medidas inéditas para regular o uso da inteligência artificial, mas com foco na propaganda eleitoral das eleições municipais de 2024. Por meio de 12 resoluções aprovadas, o TSE introduziu diversas diretrizes, incluindo a proibição de *deepfakes*, a exigência de identificação do uso de IA, restrições ao emprego de robôs para interações com eleitores, e a responsabilização das grandes empresas de tecnologia por conteúdos prejudiciais.

A fim de prevenir a propagação de desinformação durante o processo eleitoral, duas cláusulas foram adicionadas às resoluções. Elas proíbem a propagação de conteúdo falso ou manipulado, e responsabilizam as plataformas online na remoção imediata de conteúdos prejudiciais. As leis aprovadas orientam todos os que participam do processo eleitoral, incluindo partidos, candidatos, eleitores e juízes eleitorais. Além disso, prometem construir um repositório de decisões do TSE (2024) para facilitar a remoção de conteúdo falso.

6.4 SINERGIAS REGULATÓRIAS: FUNDAMENTOS PARA POLÍTICAS PÚBLICAS DO MINISTÉRIO DA DEFESA

A análise das políticas públicas e propostas de regulamentação apresentadas, incluindo aquelas relacionadas à defesa cibernética, segurança da informação e proteção de dados, revela, como uma lacuna significativa, a ausência de uma abordagem direta e específica do setor de Defesa para combater a guerra cognitiva nas redes sociais. É possível encontrar nessa sinergia

pontos de convergência e contraposição que podem ajudar a estruturar mecanismos de fortalecimento do país contra a manipulação e a desinformação nas redes sociais.

Documentos como a Política Nacional de Defesa (PND), a Estratégia Nacional de Defesa (END) e a Política Nacional de Cibersegurança (PNCiber) estabelecem diretrizes abrangentes para a proteção do espaço cibernético, mas não tratam de forma específica das ameaças psicossociais decorrentes da manipulação da cognição nas plataformas online. A PND e a END se concentram na proteção da soberania nacional e na preparação das Forças Armadas para enfrentar ameaças convencionais e cibernéticas. No entanto, essas políticas não abordam explicitamente a guerra cognitiva.

Embora esses documentos enfatizem a importância de o país estar preparado para responder a ameaças militares e cibernéticas, não tratam da disseminação de desinformação e da manipulação das percepções públicas por meio das redes sociais (Brasil, 2024b). As diretrizes priorizam principalmente aspectos físicos e cibernéticos da defesa, não abordando as dimensões psicológicas e sociais da segurança informacional. Essa ausência de diretrizes específicas para combater a guerra cognitiva é um indicativo de que o Brasil pode não estar preparado para lidar com a manipulação da opinião pública em larga escala, com consequências negativas para a coesão social e a estabilidade política e das instituições.

Entretanto, embora a PND e a END não abordem especificamente a guerra cognitiva, elas reconhecem o impacto da percepção pública nas questões de defesa. Essa percepção pode ser utilizada por agentes maliciosos para difundir histórias falsas e manipular a opinião pública. Os esforços desses normativos são complementados por outras iniciativas, como a Política Nacional de Cibersegurança (PNCiber), a Política de Inteligência de Defesa (PID), e os Projetos de Lei das *Fake News* e da Inteligência Artificial.

De igual modo, ainda que a PNCiber e a PID lidem com ameaças digitais, a guerra cognitiva envolve estratégias que vão além da proteção cibernética, incluindo aspectos psicológicos e sociais. A Doutrina Militar de Defesa Cibernética (DMDC), por sua vez, se concentra em aspectos mais amplos da defesa cibernética e segurança da informação, sem uma menção específica às redes sociais como um foco de atuação.

A implementação de medidas inovadoras, como as resoluções do TSE para regular o uso da inteligência artificial na propaganda eleitoral, oferece um modelo valioso para o desenvolvimento de políticas públicas de defesa. Outro exemplo apresentado pelo TSE, e que também pode contribuir para a elaboração de políticas públicas, é o banco de decisões do Tribunal. Esse recurso que reúne e padroniza critérios para combater a desinformação é uma ferramenta essencial e um referencial importante, pois indica os padrões de estratégias ao

observar como as informações falsas se propagam, bem como quais métodos são eficientes para combatê-las.

Os incentivos previstos nas políticas públicas e nas regulamentações podem fornecer uma base equilibrada para a formulação de uma política específica destinada a lidar com os desafios da guerra cognitiva nas redes sociais. Ao analisar as orientações delineadas em documentos como a Política Nacional de Defesa e as demais estratégias, é possível identificar lacunas e oportunidades para abordar de maneira mais abrangente as preocupações psicológicas e sociais relacionadas à segurança da informação e à influência sobre a opinião pública.

A interseção entre a segurança cibernética, a proteção da informação e a resiliência psicossocial da sociedade, delineada nesses documentos orientadores, oferece caminhos valiosos para a formulação de uma política pública que não apenas fortaleça a proteção dos sistemas de informação, mas também promova a educação digital, a capacidade crítica dos cidadãos e a transparência nas comunicações oficiais contra as ameaças da guerra cognitiva nas redes sociais. Além dos aspectos técnicos da segurança cibernética, é fundamental incluir as dimensões psicossociais envolvidas na manipulação da opinião pública e na disseminação de desinformação, considerando, nesse contexto, a Expressão Psicossocial do Poder Nacional.

Os documentos também ressaltam que é importante responder rapidamente às campanhas de desinformação. Para isso, o uso de mecanismos que permitam monitorar as atividades de agentes maliciosos na disseminação de informações enganosas é uma questão que deve ser considerada. Tais ações têm como objetivo prevenir a disseminação dessas campanhas em larga escala.

A ausência de uma política específica sobre a guerra cognitiva que aborde as questões das redes sociais pode resultar em consequências negativas para o país. Sem uma política clara, não há diretrizes eficazes para regular e monitorar o conteúdo online, facilitando a propagação de informações manipuladas. Além disso, o aumento dessas ameaças digitais deixa o país mais exposto a ataques e tentativas de desestabilização. Também existe o risco de interferência em eleições e processos democráticos, prejudicando a integridade dos sistemas políticos e influenciando a opinião pública de forma negativa. Isso pode causar desestabilização social e política, erodir a confiança nas instituições e aumentar a vulnerabilidade a campanhas promovidas por atores maliciosos, sejam eles internos ou externos. A manipulação da cognição pública contribui para potencializar as divisões sociais e políticas, criando um ambiente de desconfiança e conflito interno que pode ser explorado por adversários.

O conjunto de medidas e diretrizes para combater a manipulação da opinião pública e a disseminação de *fake news* são fundamentais para garantir a integridade das informações online

e a proteção das instituições democráticas. Além disso, uma estratégia integrada por meio de políticas públicas, facilita a coordenação entre diferentes órgãos governamentais e setores da sociedade, evitando respostas fragmentadas e ineficazes. Nesse sentido, uma abordagem coesa aumenta a eficácia dos esforços para combater as estratégias da guerra cognitiva online preservando a integridade da Expressão Psicossocial do Poder Nacional em um ambiente digital cada vez mais complexo.

6.5 DIRETRIZES PARA A ELABORAÇÃO DE POLÍTICAS PÚBLICAS DE DEFESA NACIONAL

Com a crescente disseminação da informação digital, a guerra cognitiva emerge como uma ameaça "insidiosa" à segurança nacional e à estabilidade democrática. Este capítulo buscou realizar uma análise minuciosa das estratégias e medidas necessárias para enfrentar este desafio complexo, concentrando-se na formulação de políticas públicas que fortalecem a defesa nacional contra influências maliciosas e desinformação disseminadas através de plataformas digitais.

É importante que, na abordagem das diretrizes para integrar a guerra cognitiva nas políticas de defesa, seja considerada a previsão do uso de tecnologias emergentes tanto para a detecção quanto para a mitigação de ameaças. Isso inclui ferramentas baseadas em algoritmos de IA e *big data*, que agilizam a resposta e permitem decisões precisas, automação de processos e análise eficiente de grandes volumes de dados em pouco tempo.

Além disso, também são importantes cooperações multissetoriais para fortalecer a resiliência da sociedade contra a guerra cognitiva. Essa cooperação envolve parcerias entre governos, setor privado, instituições acadêmicas e organizações da sociedade civil para compartilhar conhecimentos, recursos e melhores práticas. A interação entre esses diferentes atores não só enriquece a resposta coletiva à guerra cognitiva, mas também promove uma abordagem integrada que pode abranger desde a educação digital até a proteção de infraestruturas críticas.

No âmbito da conscientização pública, iniciativas educativas são essenciais para capacitar os cidadãos a discernir informações confiáveis de conteúdo manipulativo. Isso inclui campanhas de educação midiática que promovam a literacia digital e a consciência crítica desde a infância, preparando os cidadãos para navegar em um ambiente digital cada vez mais complexo e potencialmente enganoso.

Além dessas medidas, é necessário que sejam estabelecidas normas claras e eficazes que visem a proteção dos direitos dos indivíduos em relação a abusos e manipulações realizadas por meio das plataformas digitais. Isso envolve a transparência por parte dessas plataformas e a implementação de mecanismos de responsabilização daqueles que disseminam desinformação ou conduzem campanhas de manipulação online.

Por fim, este capítulo não apenas identifica as estratégias para enfrentar a guerra cognitiva, mas também destaca a necessidade de uma abordagem coordenada entre diversos setores, incluindo governo, setor privado, academia e sociedade civil. Essa sinergia se apresenta ainda como mais importante em um mundo interconectado onde a guerra cognitiva nas redes sociais não encontra fronteiras.

Algumas medidas essenciais incluem:

a. Incorporação à PND e END

- **Integração de estratégias contra a guerra cognitiva nas políticas de Defesa**: Incluir diretrizes específicas na Política Nacional de Defesa (PND) e na Estratégia Nacional de Defesa (END) que estabeleçam a guerra cognitiva como uma ameaça significativa, definindo estratégias para combater as campanhas, e que abranjam as redes sociais.

b. Capacitação e tecnologia

- **Criação de um centro de operações de guerra cognitiva:** Estabelecer um centro especializado, dentro do Ministério da Defesa, com equipes multidisciplinares dedicadas ao monitoramento, análise e resposta às ameaças de guerra cognitiva.

- **Desenvolvimento de capacidades tecnológicas e de inteligência:** Investir na formação de equipes especializadas em guerra cognitiva e em tecnologias de detecção de desinformação e manipulação digital. Promover o desenvolvimento de sistemas equipados com algoritmos capazes de identificar conteúdo manipulado por inteligência artificial e outras inovações tecnológicas.

- **Treinamento e capacitação de líderes:** Desenvolver e oferecer programas de treinamento e capacitação contínuos para líderes governamentais e militares sobre as dinâmicas da guerra cognitiva e as melhores práticas para enfrentá-la.

c. Cooperação e coordenação

- **Parcerias multissetoriais:** Estabelecer parcerias com plataformas de redes sociais, organizações midiáticas, instituições acadêmicas e órgãos públicos para monitorar e combater campanhas de desinformação de maneira coordenada.

- **Cooperação internacional:** Firmar acordos de cooperação estratégicos com países e organizações internacionais para o compartilhamento de melhores práticas, informações, estratégias de combate à guerra cognitiva.

d. Segurança e resiliência informacional

- **Fortalecimento da cibersegurança em plataformas críticas**: Garantir que as plataformas digitais utilizadas por instituições governamentais e de defesa tenham níveis robustos de cibersegurança para evitar que sejam utilizadas para disseminar desinformação.

e. Resposta rápida e gestão de crises

- **Desenvolvimento de protocolos de resposta rápida:** Estabelecer protocolos claros e ágeis para responder rapidamente a incidentes de guerra cognitiva, incluindo a mobilização de recursos e a comunicação com o público e parceiros estratégicos.

- **Gestão de Crises:** Desenvolver capacidades específicas no âmbito do Ministério da Defesa para gerenciar crises de desinformação – que apresenta potencial de intensificação de várias maneiras, gerando graves consequências. Estabelecer estratégias de comunicação claras, a fim de garantir respostas rápidas e coordenadas, além de promover a colaboração com parceiros relevantes.

f. Coordenação integrativa e adaptabilidade

- **Coordenação interinstitucional:** Fomentar mecanismos de coordenação entre órgãos governamentais, agências de segurança, setor privado e sociedade civil visando uma resposta integrada e eficiente às ameaças de guerra cognitiva.
- **Evolução contínua:** Implementar processos ágeis que permitam o acompanhamento da evolução das estratégias de combate à guerra cognitiva, para responder de forma eficaz a novos métodos de manipulação e desinformação.

g. Comunicação integrada e monitoramento

- **Desenvolvimento de campanhas de comunicação proativas:** Implementar iniciativas de comunicação sobre temas críticos em parceria com órgãos governamentais e sociedade civil, para se antecipar a estratégias de desinformação.

- **Monitoramento contínuo e análise de dados:** Implantar sistemas para monitoramento e análise permanente das tendências e padrões de desinformação nas redes sociais, bem como de campanhas e temas críticos.

h. Gestão e resiliência institucional

- **Avaliação de impacto e de resultados:** Incentivar a criação de mecanismos de acompanhamento e avaliação das políticas implementadas, para ajustar as estratégias e garantir que as ações realmente atinjam os objetivos desejados.

- **Resiliência Institucional:** Promover uma cultura de transparência, ética e integridade dentro das instituições governamentais, a fim de que estejam mais fortes e preparadas para enfrentar influências externas e a desinformação.

i. Desenvolvimento acadêmico e incentivo à pesquisa

- **Incentivo à pesquisa acadêmica:** Incentivar pesquisas acadêmicas permanentes sobre a guerra cognitiva por meio de colaborações entre universidades, centros de pesquisa e o setor privado para desenvolver soluções inovadoras.

j. Educação e literacia midiática

- **Educação e conscientização pública:** Implementar programas de educação digital que melhorem a alfabetização midiática e capacitem os cidadãos a reconhecer manipulações de informação e tomar decisões informadas.

k. Participação social e abordagem colaborativa

- **Participação e consulta pública:** Incluir a sociedade civil na criação e revisão de políticas públicas sobre guerra cognitiva, promovendo uma abordagem colaborativa e inclusiva.

l. Ética e responsabilidade social

- **Ética e Direitos Humanos:** Incorporar, nas estratégias contra a guerra cognitiva, princípios éticos e de respeito aos direitos humanos para garantir que sejam responsáveis e estejam dentro dos limites legais.

Diante do crescente desafio da guerra cognitiva nas redes sociais, torna-se evidente a urgência de ações coordenadas e estratégicas por parte das instituições públicas e privadas. Este subcapítulo delineou uma série de estratégias fundamentais para enfrentar as ameaças nesse ambiente, abordando desde a incorporação da guerra cognitiva nas políticas de defesa até o desenvolvimento de capacidades tecnológicas e parcerias multissetoriais. No entanto, as diretrizes apresentadas aqui oferecem um ponto de partida para a elaboração de políticas públicas eficazes neste domínio crítico da segurança.

Nesse sentido, é fundamental que o governo, organizações da sociedade civil, empresas de tecnologia e a comunidade acadêmica trabalhem em conjunto para desenvolver abordagens inovadoras e adaptáveis, que possam fazer frente às complexas dinâmicas da guerra cognitiva, a fim de proteger a integridade das instituições democráticas e garantir um ambiente online seguro e informado para todos os cidadãos.

7 CONSIDERAÇÕES FINAIS

No contexto geopolítico atual, a guerra cognitiva se apresenta como uma evolução imaterial do confronto, desafiando as concepções tradicionais de combate e abrindo um novo capítulo nos estudos militares e de segurança. As redes sociais, com seu alcance global e capacidade de propagar informações instantaneamente, se consolidam como o principal teatro de operações dessa nova guerra, onde a influência na percepção, no comportamento e na tomada de decisões de indivíduos e grupos é a arma mais letal.

Nesse novo ambiente, a disputa ocorre no campo das ideias, narrativas e representações, utilizando como principal estratégia a manipulação da percepção da realidade. Ao contrário da maioria das guerras tradicionais, que geralmente envolvem combates físicos, esse novo tipo de conflito ocorre no domínio da mente humana, explorando as vulnerabilidades do cérebro para moldar emoções, percepções e, em última instância, o comportamento, sendo capaz de desestabilizar governos e sociedades (Bernal *et al*, 2020).

A guerra cognitiva se apresenta como um dos maiores desafios da era digital particularmente no que diz respeito à disseminação de desinformação e *fake news* nas redes sociais. Nesses ambientes, a atenção e a influência são mais importantes do que a verdade, que é frequentemente relativizada, facilitando a manipulação, a distorção dos fatos e a disseminação de narrativas para influenciar a opinião pública. A "névoa digital", resultante do rápido compartilhamento de informações e da multiplicidade de fontes nesses ambientes virtuais, torna mais tênue a linha que separa os fatos verídicos dos falsificados, intensificando a complexidade dessas estratégias (Han, 2022).

Em um cenário global cada vez mais marcado pela predominância de informações digitais, a propagação de informações falsas e a fragmentação do poder nas redes sociais constituem ameaças cada vez maiores para governos e organizações. Nesse novo campo de batalha da guerra cognitiva, tanto indivíduos quanto grupos podem exercer uma influência substancial na percepção coletiva sem haja uma efetiva supervisão das instituições, resultando em um ambiente complexo e desafiador para a gestão de riscos e ameaças (Cluzel, 2020).

Considerando a complexidade desse contexto, o presente estudo foi realizado com o objetivo de oferecer subsídios para a formulação de políticas públicas pelo Ministério da Defesa contra as ameaças à Expressão Psicossocial do Poder Nacional decorrentes da guerra cognitiva nas redes sociais. Esse objetivo foi plenamente atendido por meio da metodologia aplicada, que incluiu uma revisão abrangente da literatura, análise comparativa de estudos *ex-post facto* de estratégias aplicadas nas redes sociais e a coleta e análise de dados empíricos utilizando o

método de *survey* com especialistas em defesa, segurança cibernética, psicologia social e comunicação.

Essas abordagens foram fundamentais não apenas para identificar as principais estratégias de guerra cognitiva e como esses métodos afetam os indivíduos, mas também para desenvolver recomendações práticas para elaboração de políticas públicas com diretrizes específicas que visem à proteção da Expressão Psicossocial do Poder Nacional. Entre essas recomendações, destacam-se a implementação de programas de literacia midiática e o desenvolvimento de capacidades tecnológicas para detectar e neutralizar campanhas de desinformação, além da criação de um *framework* colaborativo e da regulação das plataformas de redes sociais, para citar algumas. Com isso, o estudo não só alcançou seu objetivo principal, mas também trouxe uma contribuição importante para o campo da segurança nacional e da defesa. Ele estabelece uma base sólida para o desenvolvimento de futuras pesquisas e políticas públicas, visando gerar benefícios concretos para a sociedade.

Os objetivos específicos definidos para esta pesquisa também foram plenamente alcançados. Inicialmente, identificaram-se os vários tipos de conflito no mundo digital, com ênfase particular na guerra cognitiva online, compreendendo seus elementos centrais e como eles se manifestam no ambiente virtual. Em seguida, foram examinadas as principais estratégias empregadas por atores estatais e não estatais nos contextos das redes sociais. Esta análise destaca os principais métodos usados na guerra cognitiva, tais como a utilização de algoritmos, inteligência artificial e *digital astroturfing*; campanhas de desinformação e *fake news* polarização e divisão social; manipulação de dados pessoais; operações de influência e retórica; e recrutamento de indivíduos por grupos extremistas.

Além disso, a pesquisa investigou de que maneira as estratégias online podem influenciar a Expressão Psicossocial do Poder Nacional, oferecendo uma compreensão aprofundada dos possíveis impactos, como a erosão das instituições democráticas e do tecido social. Também foram examinadas iniciativas de políticas públicas, tanto no Brasil quanto em outros países, que visam mitigar os efeitos da desinformação nas plataformas digitais. Por fim, com base nas análises realizadas, foram apresentadas recomendações específicas para a formulação de políticas públicas pelo Ministério da Defesa, com o objetivo de enfrentar os desafios impostos pela guerra cognitiva no ambiente das redes sociais.

A investigação aprofundada das táticas de guerra cognitiva nas plataformas digitais permitiu abordar a questão principal do estudo e validar a hipótese de que campanhas de desinformação e influência nas redes sociais constituem riscos significativos para a Expressão Psicossocial do Poder Nacional. A disseminação deliberada de informações falsas, a

manipulação cognitiva da opinião pública e a promoção de narrativas divisórias são táticas identificadas como potencialmente prejudiciais à estabilidade e à coesão da sociedade.

A pesquisa *ex-post facto* sobre o uso estratégico das redes sociais como instrumento da guerra cognitiva por Estados e empresa privada, evidenciou como esses agentes têm adotado práticas coordenadas e financiadas para disseminar desinformação, distorcer fatos e promover narrativas que servem a interesses obscuros (Barnes; Sanger, 2020). A análise comparativa desses casos práticos permitiu estabelecer uma compreensão mais tangível da configuração desse novo tipo de conflito. Por outro lado, os eventos de 8 de Janeiro de 2023 evidenciaram que a sociedade brasileira é igualmente vulnerável a estratégias utilizadas nas redes sociais, que são empregadas para influenciar e fortalecer agendas políticas e especificas por meio da disseminação de desinformação e de narrativas manipuladoras.

A fragilidade do Brasil a essas ameaças se dá principalmente em decorrência da escassa literacia digital da população, da suscetibilidade social às campanhas disseminadoras de desinformação e *fake news* e da falta de regulamentação do espaço digital que possa abranger amplamente as questões relacionadas à guerra cognitiva. Essa manipulação estratégica da informação não apenas potencializou conflitos preexistentes, mas também facilitou a propagação de ideologias extremistas, demonstrando a capacidade das redes sociais de amplificar e acelerar a desestabilização sociopolítica, exacerbada pelo viés de pretenso valor patriótico (Ruediger; Grassi, 2023).

Ao demonstrar um vínculo entre a guerra cognitiva e o enfraquecimento da confiança nas instituições, este estudo abre novas frentes de pesquisa tanto no campo da defesa nacional quanto no da comunicação, da psicologia e da sociologia. No aspecto prático, os achados indicam a urgência de uma abordagem que combine diversas disciplinas para enfrentar esse desafio, propondo políticas públicas que considerem a complexidade das novas ameaças digitais. Essa abordagem deve abranger não apenas as Forças Armadas, mas também a sociedade civil e as empresas de tecnologia e *big techs,* promovendo uma resposta abrangente e coordenada.

É importante mencionar que, embora o estudo da guerra cognitiva nas redes sociais seja, indiscutivelmente, de grande relevância, ele está sujeito a certas limitações metodológicas e contextuais. O método comparativo, por exemplo, embora útil em alguns casos, não possibilita generalizar os resultados devido à dimensionalidade dos fenômenos sociais envolvidos, e à falta de controle das variáveis relevantes. Isso dificulta que as conclusões obtidas possam ser replicadas amplamente em demais casos ou contextos. Semelhantemente, a *survey,* por estar sujeita ao viés dos entrevistados, pode afetar a objetividade dos dados, comprometendo, assim,

uma análise mais racional do fenômeno. Além disso, a própria dinâmica e complexidade do tema se apresentam como fatores limitantes.

Um dos desafios identificado ao longo deste estudo foi a escassez de pesquisas específicas sobre o uso das redes sociais na guerra cognitiva no contexto brasileiro. Essa lacuna dificultou uma análise mais profunda dos mecanismos e estratégias envolvidos nas campanhas de desinformação, bem como dos métodos utilizados para combatê-las no Brasil. A situação torna-se ainda mais complexa por causa das particularidades culturais, políticas e sociais do país, que influenciam diretamente tanto a disseminação quanto os impactos da desinformação.

Além dos desafios mencionados, vale ressaltar a inovação, a complexidade e a aplicabilidade desta pesquisa, que contribui de forma significativa para a elaboração de políticas públicas no setor de defesa nacional. O estudo se destaca por explorar de maneira única e específica as ameaças à Expressão Psicossocial do Poder Nacional, decorrentes da guerra cognitiva nas redes sociais. Sendo um tema emergente e de grande relevância na atualidade, ainda existe uma necessidade de estudos específicos, o que confere a esta pesquisa um caráter original e pioneiro. A complexidade da investigação se evidencia na sua abordagem interdisciplinar, que integra conhecimentos de áreas como psicologia social, ciência da computação, segurança cibernética e comunicação. Além disso, a viabilidade das recomendações, fundamentadas em uma análise rigorosa e contextualizada das dinâmicas da guerra cognitiva, garante sua aplicabilidade na formulação de políticas públicas que respondam às constantes evoluções desse fenômeno.

Diante do exposto, reitera-se que a revisão das políticas públicas existentes mostra uma carência substancial em relação à abordagem da guerra cognitiva nas redes sociais no âmbito das diretrizes mais gerais da Política Nacional de Defesa (PND), da Estratégia Nacional de Defesa (END) e da Política Nacional de Cibersegurança (PNC). Embora esses documentos incluam a segurança do ciberespaço e o fortalecimento da Defesa contra ameaças cibernéticas e militares, eles não abordam especificamente as questões relacionadas aos riscos psicossociais da manipulação cognitiva nas redes sociais. Essa omissão pode tornar o país vulnerável a estratégias internas e externas de desestabilização cognitiva, fragilizando a segurança nacional e a confiança pública. Assim sendo, recomenda-se que o país desenvolva políticas públicas específicas que abordem essas questões, promovendo sua proteção e resiliência contra manipulações e desinformação online, garantindo, dessa forma, a integridade da Expressão Psicossocial do Poder Nacional.

REFERÊNCIAS

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (ABIN). *Terrorismo*, 23 set. 2020. Brasília; Casa Civil, Disponível em: https://www.gov.br/abin/pt-br/assuntos/fontes-de-ameacas/terrorismo Acesso em: 10 jan. 2023.

ALLCOTT, Hunt; GENTZKOW, Matthew; YU, Chuan. Trends in the diffusion of misinformation on social media. *Research & Politics*, [S.l.], v. 6, n. 2, p. 1-8, abr./jun. 2019. Disponível em: https://journals.sagepub.com/doi/10.1177/2053168019848554#body-ref-bibr6-20531680198485541. Acesso em: 31 out. 2022.

ALLCOTT, Hunt; GENTZKOW, Matthew. Social Media and Fake News in the 2016 Election. *NBER Working Paper*, No. 23089. Cambridge, MA: National Bureau of Economic Research, 2017. Disponível em: https://www.nber.org/papers/w23089. Acesso em: 31 out. 2022.

ALTHUIS, Jente; HAIDEN, Leonie (Orgs.). *Fake News: A Roadmap*. Riga: NATO Strategic Communications Centre of Excellence; King's Centre for Strategic Communications, 2018.

AMER, Karim; NOUJAIM, Jehane (Diretores). *Privacidade hackeada* [Documentário]. EUA: Netflix, 2019. Disponível em: https://www.netflix.com/br/title/80117542. Acesso em: 07 abr. 2023.

AMORIM, João Alberto Alves. *A preservação da Amazônia face ao desmatamento: cooperação e responsabilidade à luz do Direito Internacional*. 2021. Disponível em: edisciplinas.usp.br/pluginfile.php/8055015/mod_resource/content/1/A%20preserva%C3%A7%C3%A3o%20da%20Amaz%C3%B4nia%20face%20ao%20desmatamento%20%28AMORIM%202021%29.pdf. Acesso em: 27 jun. 2023.

ANCKAR, C. On the applicability of the most similar systems design and the most different systems design in comparative research. *International Journal of Social Research Methodology*, v. 11, n. 5, p. 389-401, 2008. Disponível em: tandfonline.com/doi/abs/10.1080/13645570701401552. Acesso em: 12 ago. 2023.

ANWAR, Kashif. Russia-China Information Warfare and the Changing Global Order. *The Defense Horizon Journal*, 2022. Disponível em: tdhj.org/blog/post/russia-china-information-warfare-changing-global-order/. Acesso em: 17 jun. 2022.

APPLEBAUM, Anne. China's war against Taiwan has already started. *The Atlantic*, 14 dez. 2022. Disponível em: theatlantic.com/ideas/archive/2022/12/taiwan-china-disinformation-propaganda-russian-influence/672453/. Acesso em: 2 jan. 2023.

ASEAN - ASSOCIATION OF SOUTHEAST ASIAN NATIONS. About Asean Access. *Main Portal. [*S.d.]. Disponível em: aseanaccess.com/about-us.html. Acesso em: 23 mar. 2024.

ASEAN - ASSOCIATION OF SOUTHEAST ASIAN NATIONS. AICHR-EU *Dialogue on Disinformation and Misinformation.* Singapore: 29 jan. 2024. Disponível em: eeas.europa.eu/delegations/association-southeast-asian-nations-asean/aichr-eu-dialogue-disinformation-and-misinformation_en?s=47. Acesso em: 23 mar. 2024.

ATLANTIC COUNCIL. *Undermining Ukraine: How Russia widened its global information war in 2023*. 2023. Disponível em: https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/. Acesso em: 24 jan. 2024.

BALBINO, M. L. C.; RODRIGUES, D. C. A.; FERREIRA, J. L. A.; SILVA, M. C.; SOARES, B. B. A. Inteligência artificial em Redes Sociais. *Scientia Generalis*, [S. l.], v. 2, n. Supl.1, p. 8–8, 2022. Disponível em: www.scientiageneralis.com.br/index.php/SG/article/view/221. Acesso em: 18 mar. 2022.

BARNES, Julian E.; SANGER, David E. Russian Intelligence Agencies Push Disinformation on Pandemic. *The New York Times*, 28 jul. 2020. Disponível em: www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.html. Acesso em: 12 mai. 2021.

BARRETO JUNIOR, Irineu F. *Fake News: anatomia da desinformação, discurso de ódio e erosão da democracia*. São Paulo: Saraiva Expressa Jur, 2022.

BBC NEWSNIGHT. Aleksandr Dugin: 'We have our special Russian truth'. *YouTube*, 28 out. 2016. Disponível em: www.youtube.com/watch?v=GGunRKWtWBs. Acesso em: 01 mai. 2023.

BERNAL, Alonso, et al. *Cognitive Warfare: an attack on truth and thought*. Innovation Hub, 2020. Disponível em: www.innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare.pdf. Acesso em: 12 mai. 2022.

BEAUCHAMP-MUSTAFAGA, Nathan. Cognitive domain operations: the PLA's new holistic concept for influence operations. *China Brief*, Washington D.C., The Jamestown Foundation, v. 19, n. 16, p. 1-5, set. 2019.

BIANCHI, Tiago. Internet usage in Brazil. *Statista*, 2024. Disponível em: www.statista.com/topics/2045/internet-usage-in-brazil/. Acesso em: 25 maio 2024.

BLANCO, Ignacio A.; CHAPARRO, María Ángeles D; REPISO, Rafael. El fact-checking como estrategia global para contener la desinformación. *Estudios sobre el Mensaje Periodístico*, [S.l.], v. 27, n. 3, p. 779-791, 2021. Disponível em: https://repositorio.consejodecomunicacion.gob.ec/bitstream/CONSEJO_REP/2887/1/El%20fact-checking%20como%20estrategia%20global%20para% 20contener%20la%20desinformaci%C3%B3n.pdf. Acesso em: 24 set. 2024.

BOSTROM, Nick. *Superinteligência: Caminhos, perigos e estratégias para um novo mundo*. Rio de Janeiro: DarkSide Books, 2018.

BRADSHAW, Samantha; BAILEY, Hannah; HOWARD, Philip N. *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation*. Oxford: University of Oxford, 2020. Disponível em: www.demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/02/CyberTroop-Report20-Draft9.pdf. Acesso em: 13 mai. 2023.

BRASIL. *Brasil contra fake.* Brasília: Secretaria de Comunicação Social da Presidência da República, 2023a. Disponível em: www.gov.br/secom/pt-br/fatos/brasil-contra-fake. Acesso em: 16 maio 2024.

BRASIL**.** *Ciência, Tecnologia e Inovação*. Brasília: Ministério da Defesa, 2021a. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/seprod/ciencia-e-tecnologia/ciencia-tecnologia-e-inovacao. Acesso em: 16 maio 2024.

BRASIL *Atualizada a Política de Ciência, Tecnologia e Inovação para a Defesa (PCTID).* Brasília: Ministério da Defesa, 2022a. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/seprod/ciencia-e-tecnologia/ciencia-tecnologia-e-inovacao. Acesso em: 16 maio 2024.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília: Senado Federal, 1988.

BRASIL. *De Boa na Rede.* Brasília: Ministério da Justiça, 2023b. Disponível em: https://www.gov.br/mj/pt-br/acesso-a-informacao/acoes-e-programas/deboanarede. Acesso em: 28 fev. 2024.

BRASIL. *Decreto nº 10.777, de 16 de agosto de 2021*. Aprova o Plano Nacional de Segurança Pública e Defesa Social para o período de 2021 a 2030. Brasília: Presidência da República: 2021b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10777 .htm#anexo. Acesso em: 19. Mar. 2024.

BRASIL. *Doutrina Militar de Defesa Cibernética*. 1ª Edição. 2023d. Brasília: Ministério da Defesa. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf. Acesso em: 29 abr. 2024.

BRASIL. *Estratégia Nacional de Inteligência (PNI).* Brasília: Presidência da República, 2017. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/politica-nacional-de-inteligencia-1/ENINT.pdf. Acesso em: 19 Mar. 2024.

BRASIL. *Livro Branco de Defesa Nacional*. Brasília: Ministério da Defesa, 2020c. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro_ branco_ congresso _nacional.pdf. Acesso em: 19 Mar. 2024.

BRASIL. Marinha do Brasil. *Programa de Pós-Graduação em Estudo Marítimos*. Área de Concentração e Linhas de Pesquisa. 2024c. Disponível em: https://www.marinha.mil.br/ppgem/?q=content/%C3%A1rea-de-concentra%C3%A7%C3%A3o-e-linhas-de-pesquisa . Acesso em: 19 Mar. 2024.

BRASIL. *Plano plurianual 2024-2027*: mensagem presidencial/Ministério do Planejamento e Orçamento, Secretaria Nacional de Planejamento. Brasília: Secretaria Nacional de Planejamento/MPO, 2023e.

BRASIL. *Política de Defesa Nacional*. Brasília: Presidência da República, 1996. Disponível em: http://www.biblioteca.presidencia.gov.br/publicacoes-oficiais/catalogo/fhc/politica-de-defesa-nacional-1996.pdf. Acesso em: 23 abr. 2024.

BRASIL. *Política de Inteligência de Defesa - MD60-P-01*. Brasília: Ministério da Defesa, EMCFA, 2023c. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD60P01 PolticadeIntelignciadeDefesaPID1Ed.2023.pdf. Acesso em: 29 abr. 2024.

BRASIL. *Política Nacional de Segurança da Informação da administração central do Ministério da Defesa - POSIN-MD.* Brasília: Ministério da Defesa, 2022b. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/posin-md-2022.pdf/view. Acesso em: 8 mai 2024.

BRASIL. *Política Nacional de Cibersegurança e Comitê Nacional de Cibersegurança*. Brasília: Casa Civil, 2023. https://www.planalto.gov.br/ccivil_03/ato2023-2026/2023/ decreto/D11856.htm. Acesso em: 8 mai 2024.

BRASIL. *Portaria Normativa nº9/GAP, de 13 de janeiro de 2016*. Aprova o Glossário das Forças Armadas – MD35-G-01. Glossário das Forças Armadas. 5. ed. Brasíli: Ministério da Defesa, jan. 2016.

BRASIL. *Profissionais de segurança pública são capacitados em curso voltado à defesa da democracia.* Brasília: Ministério da Justiça, 2024. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/profissionais-de-seguranca-publica-sao-capacitados-em-curso-voltado-a-defesa-da-democracia. Acesso em: 28 fev. 2024.

BRASIL. *Projeto de Lei do Senado n° 2.630, de 2020*. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Brasília: Senado Federal, 2020b. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141944. Acesso em: 17 maio 2024.

BRASIL. *Política Nacional de Defesa*. Brasília: Ministério da Defesa, Brasília: Ministério da Defesa, 2024b. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/ pnd_end _congresso_.pdf. Acesso em: 31 jan. 2024.

BRUNDAGE, Miles *et al. The Malicious use of artificial intelligence: forecasting, prevention and mitigation*. Oxford: Oxford University, 2018.

BRUNS, Axel**.** *Are filter bubbles real?* Cambridge: MIT Press, 2020.

BUCCI, Eugênio. *Desinformação e notícias falsas em período eleitoral: limites éticos e jurídicos.* Procuradoria Regional Eleitoral, 7 abr 2022. Disponível em: https://www.youtube.com/watch?v=Ou_M1rJp8SQ. Acesso em: 04 ago. 2023.

BUCCI, Francesco. S.; CRISTOFARO, Matteo; GIARDINO, Pier L. *Infodemia e pandemia: la cognitive warfare ai tempi del SARS-CoV-2,* 2023. Disponível em: https://arxiv.org/pdf/ 2308.00706. Acesso em: 23 jul. 2023.

BUZAN, Barry; WÆVER, Ole. *Regions and powers: The structure of international security*. Cambridge University Press, 2003.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. The Guardian, London, 17 mar. 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em: 23 Fev. 2021.

CÂMARA, Thiago. Terrorismo na Era da Internet: O Uso de Redes Sociais pelo Estado Islâmico. *Revista Relações Internacionais no Mundo Atual*, vol. 1, nº 21, 2016, pp. 196-221. Disponível em: https://revista.unicuritiba.edu.br/index.php/RIMA/article/view/1381/1394. Acesso em: 03 ago 2022.

CÂMARA DOS DEPUTADOS. *Câmara aprova atualização da Política Nacional de Defesa.* 15 maio 2024. Disponível em: https://www.camara.leg.br/noticias/1062814-camara-aprova-atualizacao-da-politica-nacional-de-defesa/. Acesso em: 16 mai 2024.

CAMBRIDGE ANALYTICA. *CA Political: An overview of Cambridge Analytica's political division* (Catalogue). USA: New York, 2016. Disponível em: https://ia803204.us.archive.org/35/items/ca-docs-with-redactions-sept-23-2020-4pm/FINAL-Cambridge-Analytica-Selec-20201-Campaign-Related-Documents-Redactions_.pdf. Acesso em: 23 out. 2022.

CASTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 1999.

CASTILHO, Carlos. *A guerra cognitiva ou a batalha pelo controle do nosso cérebro.* Observatório da Imprensa, edição 1231, 28 mar 2023. Disponível em: https://www.observatoriodaimprensa.com.br/comunicacao/a-guerra-cognitiva-ou-a-batalha-pelo-controle-do-nosso-cerebro/. Acesso em 9 Mai 2023.

CHAN, J. (2024). Online astroturfing: A problem beyond disinformation. *Journal of Abnormal and Social Psychology*, 62(3), 649-658.

CHOI, Hanbyul.; PARK, Jonghwa.; JUNG, Yoonhyuk. The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, v. 81, p. 42-51, 2018.

CHOUCRI, Nazli. *Cyberpolitics in International Relations***.**Cambridge: MITPress, 2012.

CLARKE, Richard. A.; KNAKE, Robert. K. *Guerra cibernética: a próxima ameaça à segurança nacional e o que fazer a respeito.* Rio de Janeiro: Brasport, 2012.

CLAUSEWITZ, Carl von. *Da Guerra*. Tradução de Magda Lopes. 2. ed. São Paulo: Martins Fontes, 1996.

CLAVERIE, Bernard; CLUZEL, François du. *Cognitive warfare: the advent of the concept of cognitics in the field of warfare*. NATO Collaboration Support Office, 2022.

CLAVERIE, Bernard; PRÉBOT, Baptiste; BUCHLER, Norbou; CLUZEL, François du. (Eds.). *First NATO scientific meeting on Cognitive Warfare (France)*. Innovation Hub of NATO-ACT and ENSC, 21 Jun 2021. Disponível em: https://innovationhub-act.org/wp-content/uploads/2023/12/Cognitive-Warfare-Symposium-ENSC-March-2022-Publication.pdf. Acesso em: 24 ago. 2022.

CLUZEL, François du. *Cognitive warfare: a new operational domain*. NATO Strategic Analysis Series, 154, 2020.

COAF - Conselho de Controle de Atividades Financeiras – Coaf. *National Risk Assessment*. Brazil, 2021. Disponível em: https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/

avaliacao-nacional-de-riscos/4-1_executive-summary_national-risk-assessment_ing.pdf. Acesso em: 7 jul. 2023.

COIMBRA, Marcos. *Operações psicológicas, corações e mentes*. Monitor Mercantil. Rio de Janeiro, 06 dez. 2007. Disponível em: https://monitormercantil.com.br/operauues-psicolugicas-nos-corauues-e-mentes/ Acesso em: 10 maio 2009.

COLE, August.; LE GUYADER, Hervé. NATO sixth's domain of operations. *In Silico: The Speech That Never Wa*s. [S.l.]: [s.n.], p. 29, 2021.

COMISSÃO EUROPEIA. Comunicação conjunta ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: *Plano de Ação contra a Desinformação.* Bruxelas, 5 Dez 2018. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX%3A52018JC0036. Acesso em: 23 Mai 2023.

CONLEY, Heather A.; ELLEHUUS, Ragnhild; KOSTELANCIK, Thomas; MANKOFF, Jeffrey; NEWLIN, Christopher; SEARIGHT, Amy; STEWART, Daniel. *Countering Russian & Chinese Influence Activities.* Center for Strategic and International Studies, 2020. Disponível em: https://www.csis.org/analysis/countering-russian-chinese-influence-activities-0. Acesso em: 23 mar. 2021.

CONGRESSO NACIONAL. Comissão Parlamentar Mista de Inquérito dos Atos de 8 de Janeiro de 2023 (Instituída pelo Requerimento nº 1, de 2023). *Relatório Final*. Brasília: Senado Federal, 2023. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9484688&ts=1697682413143&disposition=inline. Acesso em: 7 jan. 2024.

CORRÊA, Elizabeth S.; BERTOCCHI, Daniela. O Algoritmo Curador: o papel do comunicador num cenário de curadoria algorítmica de informação. *XXI Encontro Anual da Compós*, 2012.

CORRÊA, Claudio. R.; JANICK, Vinícius. R. F. *Estudos Prospectivos e Defesa no Brasil: práticas recentes e possíveis avanço*s. Economia do Mar e Poder Marítimo. 1 ed. Rio de Janeiro: Alpheratz, 2021, v. 1, p. 47-64.

COWMAN, Connor; HERNANDEZ, Aaron; SINGH, Jujhar. *Russian and Chinese influence actors and operations against the american electorate*. Global Disinformation Lab at UT Austin, 2023.

CRESWELL, John W. *Investigação Qualitativa e Projeto de Pesquisa* - 3.ed.: Escolhendo entre Cinco Abordagens. Porto Alegre: Artmed, 2014.

DĄBROWSKA, Izabela. *Maskowanie operacyjne (maskirowka) jako rosyjska zdolność zaskakiwania przeciwnika. Przegląd Bezpieczeństwa Wewnętrznego*, n. 25, 2022. Disponível em: https://www.gov.pl/web/sluzby-specjalne/maskirowka-narzedziem-rosyjskich-sil-zbrojnych. Acesso em 23. mar.2023.

DA EMPOLI, Giuliano. *Os engenheiros do caos*. Trad: Arnaldo Bloch. 1. ed. São Paulo: Vestígio, 2019.

DIESEN, Glenn. *Russia, China and the "balance of dependence" in Greater Eurasia.* Valdai Papers, 2017, disponível em https://eng.globalaffairs.ru/articles/russia-china-and-balance-of dependence-in-greater-eurasia/#_ftnref3

DIRESTA, René. et al. *The Tactics & Tropes of the Internet Research Agency*. New Knowledge, 2018. Disponível em: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1003&context=senatedocs. Acesso em: 7 jun. 2023.

DSN - DEPARTAMENTO DE SEGURIDAD NACIONAL. Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional: *Propuestas de la sociedad civil*. Gobierno de España: Solana e Hijos, 2022.

DONADIO, Rachel. *Why the Macron Hacking Attack Landed With a Thud in France.* The New York Times, 8 May 2017. Disponível em: https://www.nytimes.com/2017/05/08/world/europe/macron-hacking-attack-france.html. Acesso em: 23 Abr. 2023.

DURKHEIM, Émile. *As regras do método sociológico*. Tradução de Paulo Neves. São Paulo: Martins Fontes, 1995.

EDMUNDS, Angela; MORRIS, Anne. The problem of information overload in business organisations: a review of the literature, *International Journal of Information Management* 20, no. 1, 2000, p 17-28.

EMMERT-STREIB, Frank *et al*. An introductory review of deep learning for prediction models with big data. *Frontiers in Artificial Intelligence*, v. 3, p. 4, 2020. Disponível em: https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2020.00004/full. Acesso em: 13 ago 2023.

ENGELHAUPT, Erika. Social media crackdowns during the war in Ukraine make the internet less global. *Science News*, 23 mar. 2022. Disponível em: https://www.sciencenews.org/article/ukraine-russia-war-social-media-tiktok-telegram. Acesso em: 13 jun. 2023.

ERBSCHLOE, Michael. *Social Media Warfare*. [S.l.]:CRC Press, 2017.

ESG - ESCOLA SUPERIOR DE GUERRA. *Manual Básico: Elementos Fundamentais*. Volume I. Rio de Janeiro, 2009.

ESG - ESCOLA SUPERIOR DE GUERRA. *Fundamentos do Poder Nacional.* Rio de Janeiro, 2024.

EUROPEAN UNION. *Special Eurobarometer 477. First results. Democracy and elections.* Fieldwork, Eurobarometer, sep 2018. Disponível em: https://europa.eu/eurobarometer/surveys/detail/2198. Acesso em: 23 mai. 2023.

EUROPEAN PARLIAMENT. *Foreign Electoral Interference and Disinformation in National and European Democratic Processes* (2019/2810(RSP). European Parliament Resolution, 10 Oct 2019. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52019IP0031(01). Acesso em: 23 mai. 2023

EVANS, Geoffrey; MENON, Anand. *BREXIT and british politics.* Hoboken: John Wiley & Sons, 2017.

FARO, Leandro. 8 de janeiro no divã. *Revista Insight Inteligência*, 2023. Disponível em: https://inteligencia.insightnet.com.br/8-de-janeiro-no-diva/. Acesso em: 15 jan 2024.

FIELD, Hayden; VANIAN, Jonathan. *Tech layoffs ravage the teams that fight online misinformation and hate speech*. CNBC, 26 may 2023. Disponível em: https://www.cnbc.com/2023/05/26/tech-companies-are-laying-off-their-ethics-and-safety-teams-.html. Acesso em: 31 mai 2023.

FISAS, Vicenç. *Cultura de Paz y Gestão de Conflitos*, Paris: Ediciones UNESCO, 2004.

FLICK, Uwe. *Introdução à pesquisa qualitativa*. 3. ed. Porto Alegre: Artmed, 2009.

GELFERT, Axel. *Fake News: A Definition. Informal Logic* 38. 2018, 84-117. Disponível em: https://informallogic.ca/index.php/informal_logic/article/view/5068. Acesso em: 15 jan 2023.

GERHARDT, Tatiana E.; SILVEIRA, Denise T. (org.). *Métodos de pesquisa*. Porto Alegre: Editora da UFRGS, 2009.

GEERS, Kenneth. *Cyber War in Perspective: Russian Aggression Against Ukraine*. NATO CCDCOE Publications: Tallinn, 2015.

GIL, Antônio Carlos. *Métodos e técnicas de pesquisa social*. 5. ed. São Paulo: Atlas, 1999.

GILES, Keir; JOHNSON, Matthew D.; NAZAROV, Mykola; STOICESCU, Kalev. *How Russia went to war: the Kremlin's preparations for its aggression against Ukraine.* International Centre for Defence and Security (ICDS), 2023. Disponível em: https://icds.ee/wp-content/uploads/dlm_uploads/2023/04/ICDS_Report_How_Russia_Went_to_War_Stoicescu_Nazarov_Giles_Johnson_April_2023.pdf Acesso em: 4 out. 2023.

GREENBERG, Andy. Sandworm: *Uma Nova Era na Guerra Cibernética e a Caça pelos Hackers mais Perigosos do Kremlin*. Rio de Janeiro: Editora Brasport, 2022.

GOBIERNO DE ESPAÑA. *Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional: Propuestas de la sociedad civil*. España: Presidencia del Gobierno, 2022 Disponível em https://www.dsn.gob.es/sites/dsn/files/LibroDesinfoSN.pdf. Acesso em: 23 ago 2023.

G1. '*Le Monde' anuncia decisão de não publicar conteúdo de documentos hackeados da campanha de Macron.* 06 Mai 2017. Disponível em: https://g1.globo.com/mundo/eleicoes-na-franca/2017/noticia/le-monde-anuncia-decisao-de-nao-publicar-conteudo-de-documentos-hackeados-da-campanha-de-macron.ghtml. Acesso em: 08. Mai 2022.

G7. *G7 Rapid Response Mechanism*: *Protecting Democracy*. Annual Report 2022. Canadá. Disponível em: https://www.international.gc.ca/transparency-transparence/assets/pdfs/rapid-response-mechanism-mecanisme-reponse-rapide/g7-rrm-2022-annual-report-en.pdf. Acesso em: 9 jan 2024.

G20. *Instituições científicas brasileiras anunciam iniciativa contra desinformação e discurso de ódio durante evento do G20*. 30 Abr 2024. Disponível em: https://www.g20.org/pt-br/noticias/instituicoes-cientificas-brasileiras-anunciam-iniciativa-contra-desinformacao-e-discurso-de-odio-durante-evento-do-g20. Acesso em: 8 maio 2024.

HAN, Byung-Chul. *Infocracia: digitalização e a crise da democracia.* Tradução de Gabriel S. Philipson. Editora Vozes, 2022.

HAROLD, Scott W; BEAUCHAMP-MUSTAFAGA, Nathan; HORNUNG, Jeffrey W. *Chinese disinformation efforts on social media*. Santa Monica, CA: RAND Corporation, 2021.

HOWARD, Michael. *The Causes of Wars*. 2. ed. Cambridge, MA: Harvard University Press, 1984.

HERRERA, Fidel C. *O impacto da liderança de Mao na China ainda está vivo e próspero*. Revista Profissional da Força Aérea dos EUA, [S.l.], segunda edição 2022, p. 107-1111. Disponível em: https://www.airuniversity.af.edu/Portals/10/JOTA/journals/Volume-4_Issue-2/04-Castro_port.pdf. Acesso em: 18 jun. 2023.

HENRIQUE, Layane. *Reunião do G7: o que os países mais industrializados planejam*. Politize!, 17 mai 2023. Disponível em: www.politize.com.br/reuniao-do-g7/. Acesso em: 10 set 2023.

HENRY, Charlotte. *Not buying it*. London: Unbound, 2019. E-book.

HOLLOWAY, Michael. *How Russia Weaponized Social Media in Crimea*. The Strategy Bridge, 10 maio 2017. Disponível em: https://thestrategybridge.org/the-bridge/2017/5/10/how-russia-weaponized-social-media-in-crimea. Acesso em: 12 jul. 2023.

HOUSE OF COMMONS. *Disinformation and 'fake news': Interim Report*. London: House of Commons, 2019. Disponível em: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179104.htm. Acesso em: 24 set. 2022.

HUGHES, Heather. C.; WAISMEL-MANOR, Israel. *The macedonian fake news industry and the 2016 us election.* PS: Political Science & Politics, Volume 54, Número 1, 25 ago de 2020. Editora: Cambridge University Press.

HUNG, Tzu-Chieh; HUNG, Tzu-Wei. How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars. *Journal of Global Security Studies*, v. 7, n. 4, p. 1-18, 2020. Disponível em: https://doi.org/10.1093/jogss/ogac016. Acesso em: 23 out. 2023.

HUNTINGTON, Samuel. *O choque das civilizações e a reconstrução da ordem mundial.* Rio de Janeiro: Objetiva, 1997.

IBGE - INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. O Brasil no mundo. In: *IBGE Educa Crianças.* [S. l.], 2023. Disponível em: https://educa.ibge.gov.br/criancas/brasil/nosso-territorio/19638-o-brasil-no-mundo.html. Acesso em: 27 jul. 2024.

IBM**.** *Phishing: O que é e como se proteger*. 2023a. Disponível em: https://www.ibm.com/br-pt/topics/phishing. Acesso em:10 jan. 2024.

IBM**.** *O que é engenharia social*. 2023b. Disponível em: https://www.ibm.com/br-pt/topics/social-engineering. Acesso em:10 jan. 2024.

INTELLIGENCE COMMUNITY ASSESSMENT. *Assessing russian activities and intentions in recent US elections.* 6 jan. 2017. Disponível em: https://www.dni.gov/files/documents/ICA_2017_01.pdf. Acesso em: 13 jun. 2023.

INSTITUTO DE TECNOLOGIA DE MASSACHUSETTS. *Study: on Twitter, false news travels faster than true stories*. EUA: MIT, 2018. Disponível em: https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308. Acesso: 16/03/2022.

IPEA – INSTITUTO DE PESQUISA ECONÔMICA APLICADA. *Catálogo de políticas públicas: Defesa Nacional.* 2023a. Disponível em: https://catalogo.ipea.gov.br/area-tematica/2/defesa-nacional. Acesso em: 06 abr. 2024.

IPEA – INSTITUTO DE PESQUISA ECONÔMICA APLICADA. *Catálogo de políticas públicas: O que é.* 2023b. Disponível em: https://catalogo.ipea.gov.br/area-tematica/2/defesa-nacional. Acesso em: 06 abr. 2024.

ISAAK, Jim; HANNA, Mina J. *User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection.* Computer, vol. 51, n. 8, pp. 56-59, agosto de 2018. Disponível em: https://www.computer.org/csdl/magazine/co/2018/08/mco2018080056/13rRUxbCbmn. Acesso em: 21 set. 2021.

JAITNER, Margarita; MATTSSON, Peter. A. Russian Information Warfare of 2014. In: *7th International Conference on Cyber Architectures in Cyberspace*, 2015. Disponível em: https://ccdcoe.org/uploads/2018/10/Art-03-Russian-Information-Warfare-of-2014.pdf. Acesso em: 20 ago. 2022.

JENKINS, Henry; FORD, Sam.; GREEN, Joshua. *Spreadable media: creating value and meaning in a networked culture.* EUA: NYU Press, 2013.

JOHN, Jennifer N. Porque a Geração Z cai na desinformação online. *MIT Technology Review*, 26 Jun 2021. Disponível em: https://mittechreview.com.br/por-que-a-geracao-z-cai-na-desinformacao-online/. Acesso em: 21 set. 2022.

JOHNSON, Deborah G.; REGAN, Priscilla M. *Transparency and Accountability in Political Microtargeting*. In: TADDEO, Mariarosaria; FLORIDI, Luciano (ed.). The Ethics of Information Transparency. Cham: Springer, 2014. p. 161-177.

JOPLING, Michael. *Countering Russia`s Hybrid Threat: an Update. Bruxelas*: Committee on the Civil Dimension of Security, NATO Parliamentary Assembly, 2018. Disponível em: https://www.nato-pa.int/download-file?filename=sites/default/files/201812/166%20CDS%2018%20E%20fin%20-%20HYBRID%20THREATS%20%20JOPLING_0.pdf. Acesso em: 5 jan 2022.

JUNQUEIRA, Fernanda C.; FERREIRA FILHO, Edson P.; LOPES, Paloma L.; SOUSA, Elis R. R.; FONSECA, Lourrana T. A utilização das redes sociais para o fortalecimento das organizações. In: *XI Simpósio de Excelência em gestão e tecnologia*, 2014. Disponível em: https://www.aedb.br/seget/arquivos/artigos14/22020181.pdf. Acesso em: 19 jan. 2024.

KAISER, Brittany. *Manipulados: a ascensão e queda da Cambridge Analytica e o futuro da democracia.* Rio de Janeiro: Harper Colins, 2020.

KAKUTANI, Michiko. *A morte da verdade: notas sobre a mentira na era Trump*. 1. ed. Rio de Janeiro: Intrínseca, 2018. 272 p.

KANNENBERG, Fernanda; ORTELLADO, Pablo. *Fake news nas eleições de 2018 e os desafios para 2020.* Política Hoje, v. 29, n. 1, p. 54-71, 2020.

KANTAYYA, Shalini. *Coded Bias*. 24 out 2022. Netflix. 1h 30min. Documentário. Direção: Shalini Kantayya. Roteiro: Shalini Kantayya.

KELTON, Maryanne; SULLIVAN, Michael; BIENVENUE, Emily; ROGERS, Zac. *Australia, the Utility of Force and the Society-Centric Battlespace*. *International Affairs*, v. 95, n. 4, p. 859-876, 2019.

KLAYMAN, Joshua. (1995). *Varieties of Confirmation Bias*. Psychology of Learning and Motivation, 32, 385–418.

KORYBKO, Andrew. *Guerra Híbrida: das revoluções coloridas aos golpes*. 1. ed. rev. São Paulo: EDITORA EXPRESSÃO POPULAR LTDA, 2018. Disponível em: http://resistir.info/livros/guerras_hibridas.pdf. Acesso em: 7 ago. 2022.

KUX, Dennis. *Soviet active measures and disinformation: overview and assessment.* Parameters 15, no. 1, p 19. 1985.

LANHAM, Richard A. *The Economics of Attention: Style and Substance in the Age of Information.* EUA: University of Chicago Press, 2006.

LASSWELL, Harold D. *Propaganda technique in World War I*. Cambridge: MIT Press, 1971. 268 p.

LAZAROTTO, Bárbara R. The Grass is not always greener on the other side: the use of digital astroturfing to spread disinformation and the erosion of the rule of law. *LSU Law Journal for Social Justice & Policy*, 3, 2023. Disponível em: https://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=1031&context=jsjp. Acesso em: 13 abr. 2023.

LAZER, D. M. et al. The science of fake news. *Science*, v. 359, n. 6380, p. 1094-1096, 2018.

LI, Linda.; VASARHELYI, Orsolya; VEDRES, Balazs. *Social bots sour activist sentiment without eroding engagement.* Cornell University, 2024. Disponível em: https://arxiv.org/abs/2403.12904. Acesso em: 06/02/2023.

LIJPHART, A. (1971). Comparative Politics and the Comparative Method. *The American Political Science Review,* 65(3), 682-693. Disponível em: http://www.jkarp.com/s2008/ Lijphart.pdf. Acesso em: 12 mar. 2023.

LUKES, Steven. *Power: a radical view*. London: Macmillan, 1974.

MCMILLAN, James H, SCHUMACHER, Sally. *Research in Education: Evidence-Based Inquiry.* Boston, MA: Pearson/Allyn and Bacon, 2006.

MAHBUBANI, Kishore. Power Shifts, Economic Change and the Decline of the West? *International Relations of the Asia-Pacific*, vol. 13, no. 3, 2013, pp. 299-319.

MARCONI, Marina. de A.; LAKATOS, Eva M. *Fundamentos de Metodologia Científica*. 5ª ed. São Paulo: Atlas, 2003.

MERRIAM-WEBSTER. *The Real Story of 'Fake News'* (2024). Disponível em: https:// www.merriam-webster.com/wordplay/the-real-story-of-fake-news. Acesso em: 24 set. 2023.

MIIKKULAINEN, Risto. Generative AI: an AI paradigm shift in the making? *AI Magazine*, 45, 165-167. Aceito para publicação em 6 de outubro de 2023. Disponível em: https://www.researchgate.net/publication/378293472_Generative_AI_An_AI_paradigm_shift _in_the_making/link/664a4a9b479366623afd29d4/download. Acesso em: 13 maio 2024.

MOLTER, Vanessa; DIRESTA, Renee. *Pandemics & propaganda: how Chinese state media creates and propagates CCP coronavirus narratives*. Stanford, 2020. Disponível em: https://cyber.fsi.stanford.edu/io/publication/pandemics-propaganda. Acesso em 18 fev 2022.

MONNERAT, Alessandra. *2 anos de Guerra na Ucrânia: relembre 8 narrativas de desinformação sobre o conflito*. Estadão Verifica, 24 fev 2024. Disponível em: https://www.estadao.com.br/estadao-verifica/2-anos-de-guerra-na-ucrania-relembre-8-narrativas-de-desinformacao-sobre-o-conflito/. Acesso em: 2 abr. 2024.

MORAIS, Flávio. D. B. de; BRANCO, Valdec. R. C. A inteligência artificial: conceitos, aplicações e controvérsias. In: *XX Simpósio Internacional de Ciências Integradas da Unaerp*, Campus Guarujá. 2022. Disponível em: https://www.unaerp.br/documentos/5528-a-inteligencia-artificial-conceitos-aplicacoes-e-controversias/file. Acesso em: 22 jan. 2023

MORENO, Alberto P. La Evolución del Terrorismo de Al Qaeda al ISIS: Organización, Metodología y Perfiles. *Razón y Fe*, vol. 279, no. 1437, 2019, pp. 35-48. Disponível em: file:///C:/Users/gnich/AppData/Local/Temp/MicrosoftEdgeDownloads/0cfd6550-b9c6-479d-bb20-46373754c7e3/terro.pdf. Acesso em: 14 mai. 2023.

MORGENTHAU, Hans J. *A Política entre as Nações: A Luta pela Guerra e pela Paz*. Brasília: Editora Universidade de Brasília, 2003. Disponível em: https://funag.gov.br/loja/download/ 0179_politica_entre_as_nacoes.pdf. Acesso em: 23 abr. 2023.

MORRIS, Shane; GURZICK, David, Ph.D.; GUILLORY, Sean, Ph.D.; BORSKY, Glenn. Countering Cognitive Warfare in the Digital Age: *A Comprehensive Strategy for Safeguarding Democracy against Disinformation Campaigns on the TikTok Social Media Platform.*

Information Professionals Association, 2024. Disponível em: https://information-professionals.org/countering-cognitive-warfare-in-the-digital-age/. Acesso em: 20 jun. 2024.

MOULAS, Dimitris; BOATENG, Nana. *The new dimension of cognitive warfare: Procedures implemented to innovate and defend against adversaries*. In: NATO Innovation Network Conference, 9 Nov 2021, Proceedings. Session: Open Innovation - Cognitive Warfare Use Case. [Online]. Disponível em: https://innovationhub-act.org/wp-content/uploads/2023/12/Open-Innovation-Cognitive-Warfare.pdf. Acesso em: 10 abr. 2024.

MUELLER, Robert. S. *Report on the investigation into russian interference in the 2016 presidential election*. Washington, DC: U.S. Department of Justice, 2019.

MURPHY, Frank. *Reality of War Should Define Information Warfare*. Proceedings, mar. 2021. Disponível em: https://www.usni.org/magazines/proceedings/2021/march/reality-war-should-define-information-warfare. Acesso em: 30 jan. 2022.

NAÍM, Moisés. *O fim do poder: como as novas e múltiplas formas de poder estão mudando o mundo*. Rio de Janeiro: Leya, 2014.

NATO Review. *Countering cognitive warfare: awareness and resilience*, 2021. Disponível em: https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html

NATO (OTAN). *Multi-domain operations in NATO*. Allied Command Transformation, 5 out. 2023. Disponível em: https://www.act.nato.int/activities/multi-domain-operations/. Acesso em: 12 fev. 2022.

NATO (OTAN). *NATO Warfighting Capstone Concept (NWCC).* 2021. Disponível em: https://www.act.nato.int/wp-content/uploads/2023/06/NWCC-Glossy-18-MAY.pdf. Acesso em: 18 jun 2022.

NATO (OTAN). *NATO 2022 strategic concept* adopted by heads of state and government at the NATO Summit in Madrid, 29 Jun 2022a. Disponível em: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf. Acesso em: 18 jun 2022.

NATO (OTAN). *NATO STO to hold workshop on cognitive warfare.* Nov 2022. Disponível em: https://www.sto.nato.int/Lists/STONews Archive/displaynewsitem.aspx?ID=710. Acesso em: 05.jan.2023

NICHOLS, Giselli C. L.; CORRÊA, Claudio R. A guerra cognitiva nas redes sociais e suas implicações para a segurança dos Estados. *Revista da Escola Superior de Guerra*, v. 38, n. 82, 04 dez. 2023. Disponível em: https://revista.esg.br/index.php/revistadaesg/article/view/1297. Acesso em: 19 fev 2024.

NOUWENS, Meia. *China's New Information Support Force*. IISS, 03 mai 2024. Disponível em: https://www.iiss.org/online-analysis/online-analysis/2024/05/chinas-new-information-support-force/. Acesso em: 10 mai. 2024.

NYE JR, Joseph S. *Soft Power: The Means to Success in World Politics*. EUA: PublicAffairs Books, 2005.

NYE JR, Joseph S. *O Futuro do Poder*. São Paulo: Editora Campus, 2012.

NYE JR, Joseph S. *O paradoxo do poder Americano: porque a única superpotência do mundo não pode prosseguir isolada.* São Paulo: Editora UNESP, 2002.

OEA – ORGANIZAÇÃO DOS ESTADOS AMERICANOS. *Declaração conjunta do vigésimo aniversário: desafios para a liberdade de expressão na próxima década*. Relatoria Especial para a Liberdade de Expressão da CIDH, 2019. Disponível em: www.oas.org/pt/cidh/ expressao/showarticle.asp?artID=1146&lID=4. Acesso em: 23 Ago 2023.

O´NEIL, Cathy. *Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia*. Tradução Rafael Abraham. 1. ed. Santo André, SP: Editora Rua do Sabão, 2020.

ONU - ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression***.** Nova Iorque, 16 Mai 2011. Disponível em: http://www2.ohchr.org/english/bodies/hrcouncil/docs/ 17session/ A.HRC.17.27_en.pdf. Acesso em: 10 Jul. 2022.

ONU - ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Princípios Orientadores sobre Empresas e Direitos Humanos (POs)*. Brasil, 2019. Disponível em: https://www.gov.br/mdh/pt-br/assuntos/noticias/2019/outubro/Cartilha_versoimpresso.pdf. Acesso em: 23 Set. 2023.

ORENSTEIN, Harold. Apresentação de 2018 do Chefe do Estado-Maior Geral Russo Valery Gerasimov". *Army University Press*, 2019. Disponível em: https://www.armyupress.army.mil/ Portals/7/military-review/Archives/Portuguese/Online%20Exclusives/Gerasimov-Apresentacao-de-2018-do-Chefe-do-Estado-Maior-Geral-Russo-Valery-Gerasimov-POR-OLE-Jan-2019.pdf. Acesso em: 21 mar. 2022.

ORLOWSKI, Jeff. *O Dilema das Redes*. Direção. Netflix, 2020. 1h 34min. Disponível em: https://www.netflix.com/br/title/81254224. Acesso em: 29 mar 2022.

OXFORD LEARNER'S DICTIONARIES. *Post-truth.* [s.d.]. 2016. Disponível em: https://www.oxfordlearnersdictionaries.com/us/definition/english/post-truth?q=post+truth. Acesso em: 21 fev 2023.

OZAWA, João V. S. et al. *How Disinformation on WhatsApp Went From Campaign Weapon to Governmental Propaganda in Brazil*. The International Journal of Press/Politics, [S.l.], v. 26, n. 2, p. 315-334, 2021. Disponível em: https://journals.sagepub.com/doi/full/10.1177/ 20563051231160632. Acesso em: 4 jun. 2023.

PARISER, Eli. *The Filter Bubble: What the internet is hiding from you*. New York: The Penguin Press, 2011. E-book.

PARKS, Raymond C.; DUGGAN, David P. *Principles of cyberwarfare.* IEEE Security & Privacy, v. 9, n. 5, p. 30-35, 2011.

PETTICREW, Mark; ROBERTS, Helen. *Systematic Reviews in the Social Sciences: A Practical Guide.* Oxford: Blackwell Publishing, 2006.

PIJPERS, Peter B.M.J., VOSKUIJL Mark; BEERE, Robert J.M. (eds.). *Towards a Data-Driven Military: A Multidisciplinary Perspective*. Leiden University Press, 2022.

PINHEIRO, Petrilson. *Fake news em jogo: uma discussão epistemológica sobre o processo de produção e disseminação de (in) verdades em redes sociais.* São Paulo: Delta – PUC, 2021. Disponível em: https://www.scielo.br/j/delta/a/8gjBC9zP3Xt3rNJbdzpPPhb/?format=pdf&lang=pt. Acesso em: 23 Mar 2023.

PRZEWORSKI, Adam; TEUNE, Henry. *The Logic of Comparative Social Inquiry*. New York: Wiley-Interscience, 1970.

PUTNAM, R. *Comunidade e Democracia: a experiência da Itália Moderna*. 2. ed., Rio de Janeiro: FGV, 2005.

QUANDT, Thorsten; FRISCHLICH, Lena; BOBERG, Svenja; SCHATTO-ECKRODT, Tim. Fake News. *In: Encyclopedia of Social Network Analysis and Mining.* 2019, p.1-6). Disponível em: https://www.researchgate.net/publication/332749986_Fake_News. Acesso em: 13 Mar 2023.

RED DIAMOND. Operational Environment and Threat Analysis Directorate. Chinese Information Operations. *Red Diamond Newsletters*, [S.l.], 2021. Disponível em: https://community.apan.org/wg/tradoc-g2/operational-environment-and-threat-analysis-directorate/w/red-diamond-newsletters/34323/4-chinese-information-operations/. Acesso em: 9 jan. 2023.

RÊGO, Ana R.; BARBOSA, Marialva. *A construção intencional da ignorância*. Rio de Janeiro: Editora Mauad, 2020.

REHMAN, Ikhlaq ur. *Facebook-Cambridge Analytica data harvesting: What you need to know.* 2019. Library Philosophy and Practice (e-journal). Disponível em: https://core.ac.uk/download/pdf/220153793.pdf. Acesso em: 15 jun 2022.

RICARD, Julie; MEDEIROS, Juliano. Using misinformation as a political weapon: COVID-19 and Bolsonaro in Brazil. *Harvard Kennedy School Misinformation Review*, 1(3), Article 13. 17 abr. 2020 Disponível em: https://doi.org/10.37016/mr-2020-013. Acesso em: 13 ago 2021.

RID, Thomas. *Cyber War Will Not Take Place*. Oxford University Press, 2013.

RIDOLFO, Jim; HART-DAVIDSON, William. *Rhet Ops: Rhetoric and In; formation Warfare*. EUA: University of Pittsburgh Press, 2019.

RINI, R. *Fake News and Partisan Epistemology*. Kennedy Institute of Ethics Journal, 2017. Disponível em: https://kiej.georgetown.edu/fake-news-partisan-epistemology/. Acesso em: 23 mai. 2023.

RODRÍGUEZ, Nunes. A Guerra pela mente do público. *Revista Profissional da Força Aérea dos EUA*, Primeira Edição 2020. Disponível em: https://www.airuniversity.af.edu/Portals/10/JOTA/Journals/Volume%202%20Issue%201/02-Rodriguez_port.pdf. Acesso em: 13 mai. 2023.

ROTHKOPF, David J. *When the Buzz Bites Back*. Washington Post, [S.l.], 11 maio 2003. Disponível em: https://www.washingtonpost.com/archive/opinions/2003/05/11/when-the-buzz- bites-back/bc8cd84f-cab6-4648-bf58-0277261af6cd/. Acesso em 24 mai.2023.

ROUSSEAU, Jean. J. *Do contrato social.* São Paulo: Martin Claret, 2013.

RUEDIGER, Marco Aurelio; GRASSI, Amaro**.** *Ataque à democracia e repercussão do dia 8 de janeiro:* disputas narrativas em torno dos atos antidemocráticos nas plataformas on-line. Rio de Janeiro: FGV ECMI, 2023.

RUSSELL, Stuart; NORVIG, Peter. *Artificial Intelligence: A Modern Approach*. 3. ed. Upper Saddle River: Prentice Hall, 2010.

SANTAELLA, Lucia. *A pós-verdade é verdadeira ou falsa?* São Paulo: Estação das Letras e Cores, 2018.

SÁNCHEZ, Juan L.M.; RUIZ, María J. U. *Algoritmos y bots aplicados al periodismo. El caso de Narrativa Inteligencia Artificial: estructura, producción y calidad informativa.* Doxa Comunicación, vol. 29, 2019.

SÁNCHEZ, Juan L. M.; RUIZ, Maria J. U. Inteligencia artificial y periodismo: una herramienta contra la desinformación. *Revista CIDOB d'Afers Internacionals*, (124), 49-72, 2020. Disponível em: https://www.cidob.org/publicaciones/inteligencia-artificial-y-periodismo-una-herramienta-contra-la-desinformacion. Acesso em: 13 mar. 2021.

SANGER, David E. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York: Crown Publishing, 2018.

SEAVER, Nick. *Algorithmic recommendations and synaptic functions*. Limn. n.2. 2012.

SEIBT, Taís. *Checagem governamental é bem-vinda, se tiver base em fatos.* Desinfomante, 2023. Disponível em: https://desinformante.com.br/governos-checagem-de-fatos. Acesso em: 23 set. 2023

SETTLE, Jaime. *Frenemies: How Social Media Polarizes America*. Cambridge, MA: Cambridge University Press, 2018.

SCHUDSON, Michael. *Como saber se uma notícia é falsa?* Observatório da Imprensa, [S. l.], 2017. Disponível em: https://www.observatoriodaimprensa.com.br/edicao-brasileira-da-columbia-journalism-review/como-saber-se-uma-noticia-e-falsa/. Acesso em: 3 set. 2023.

SILVA, Antonio Henrique Lucena. A China e o seu processo de modernização militar. *Revista Defesa e Segurança*, v. 2, p. 207-213, 2016.

SINGER, Peter. W.; BROOKING, Emerson T. *LikeWar: The Weaponization of Social Media.* Boston: Houghton Mifflin Harcourt, 2018.

SOLDATOV, Andrei; BOROGAN, Irina. *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*. Nova York: PublicAffairs, 2015.

SOLON, Olivia. *Facebook says Cambridge Analytica may have gained 37m more users' data*. The Guardian, 4 Apr 2018. Disponível em: https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought. Acesso em: 13 jul. 2023.

SORJ, Bernardo; CRUZ, Francisco B.; SANTOS, Maike W.; RIBEIRO, Marcio M., ORTELLADO, Pablo. *Sobrevivendo nas redes: guia do cidadão*. São Paulo: Moderna, 2018.

SOUZA, Devilson R.; GORCZEVSKI, Clóvis. A manipulação das informações e o perigo à democracia: a ameaça oferecida pelo acesso irrestrito a dados pessoais. *Revista de Direito Brasileira*. Florianópolis, SC, v. 26, n. 10, p. 410-423, Mai./Ago. 2020.

SPAULDING, Suzanne; NAIR, Devi. *Institutional integrity: learning the right lessons from the Capitol siege.* Center for Strategic and International Studies (CSIS), 2021. Disponível em: https://www.csis.org/analysis/institutional-integrity-learning-right-lessons-capitol-siege. Acesso em: 24 jul. 2023.

SKOVE, Sam. (2024). *How Army special operators use deepfakes and drones to train for information warfare.* Defense One. Disponível em: https://www.defenseone.com/technology/2024/04/how-army-special-operators-use-deepfakes-and-drones-train-information-warfare/395852/. Acesso em: 18 abr. 2024.

STASSUN, Cristian Caê Seemann; ASSMANN, Selvino José. Hipermobilidade estética e dispositivos de controle de circulação: o desejo de ser notado e encontrado na internet. *Cadernos de Pesquisa Interdisciplinar em Ciências Humanas*, v. 13, n. 102, p. 153-168, 2012. Disponível em: https://periodicos.ufsc.br/index.php/cadernosdepesquisa/article/view/1984-8951.2012v13n102p153. Acesso em: [data de acesso].

SUBRAMANIAN, Samanth. *Inside the macedonian fake-news complex*. Wired, 15 fev. 2017. Disponível em: https://www.wired.com/2017/02/veles-macedonia-fake-news. Acesso em 30 set. 2023.

SUPREMO TRIBUNAL FEDERAL. *Programa de Combate à Desinformação*. Brasília: STF, 2021. Disponível em: https://portal.stf.jus.br/desinformacao/#sobrePCD. Acesso em: 01 jan. 2024.

SUN TZU ART OF WAR. *Who is Sun Tzu? A brief introduction to Sun Tzu's Life*?. 2023. Disponível em: https://suntzuartofwar.org/who-is-sun-tzu/. Acesso em: 31 mar. 2024.

SYED, Ghazi. S.; ZHOU, Yingqiu; WARNER, Jamie.; BHASKARAN, Harish. *Atomically thin optomemristive feedback neurons*. 2023. Nature Nanotechnology. Disponível em: https://www.nature.com/articles/s41565-023-01391-6. Acesso em: 13 ago. 2023.

TARDÁGUILA, Cristina. *Brasil contra fake não linka fonte ou cita só o governo em 52% das 'checagens'*. Lupa, 24 nov. 2023. Disponível em: https://lupa.uol.com.br/jornalismo/2023/11/24/brasil-contra-fake-nao-linka-fonte-ou-cita-so-o-governo-em-52-das-checagens. Acesso em: 03 jan. 2024.

TOFFLER, Alvin. *Future shock.* New York: Random House; 1970.

TOLEDO, Marcelo. *Bolsonaristas falam em Deus e fazem atos golpistas em diferentes cidades do país.* Folha de S. Paulo, 02 Nov 2022. Disponível em: https://www1.folha.uol.com.br/poder/2022/11/bolsonaristas-falam-em-deus-e-fazem-atosgolpistas-em-diferentes-cidades-do-pais.shtml. Acesso em: 03 Mai 2023.

TRIVIÑOS, Augusto N. S. *Introdução à pesquisa em ciências sociais: a pesquisa qualitativa em educação.* São Paulo: Atlas, 1987.

TSE - TRIBUNAL SUPERIOR ELEITORAL. Programa Permanente de Enfrentamento à Desinformação no Âmbito da Justiça Eleitoral. *Relatório de Ações e Resultados.* Eleições 2022**.** TSE, 2023. Disponível em: https://www.justicaeleitoral.jus.br/ desinformacao/arquivos/ programa-permanente-de-enfrentamento-a-desinformacao-novo.pdf. Acesso em: 02 fev. 2024.

TSE - TRIBUNAL SUPERIOR ELEITORAL. *TSE proíbe uso de inteligência artificial para criar e propagar conteúdos falsos nas eleições*. 2024. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2024/Fevereiro/tse-proibe-uso-de-inteligencia-artificial-para-criar-e-propagar-conteudos-falsos-nas-eleicoes. Acesso em: 13 de junho de 2024.

TZU, Sun. *A Arte da Guerra: os treze capítulos originais*. Trad. André da Silva Bueno. São Paulo: Jardim dos Livros, 2017.

UNDERWOOD, Kimberly. *Cognitive warfare will be deciding factor in battle*. Armed Forces Communications & Electronics Association International, [S.l], 2017. Disponível em: https://www.afcea.org/signal-media/cyber/cognitive-warfare-will-be-deciding-factor-battle. Acesso em: 15 jun 2023.

UNESCO. *Guidelines for the Governance of Digital Platforms: Safeguarding freedom of expression and access to information through a multistakeholder approach*. Paris: United Nations Educational, Scientific and Cultural Organization, 2023. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000387339/PDF/387339eng.pdf.multi. Acesso em: 12 Dez 2023.

VASWANI, Ashish et al. *Attention is All You Need*. In: Neural Information Processing Systems, 30., 2017, Long Beach. Proceedings [...]. Long Beach: NIPS, 2017. Disponível em: https://papers.nips.cc/paper_files/paper/2017/hash/3f5ee243547dee91fbd053 c1c4a845aa-Abstract.html. Acesso em: 12 jul. 2024.

VIOLA, Eduardo; LIMA, Jean. *Desafios para a ascensão chinesa no Sistema Internacional de Hegemonia das Democracias de Mercado*. Carta Internacional, Vol. 8, n. 2, Jul-Dez 2013, p. 116-136).

VISACRO, Alessandro. *A guerra na era da informação*. São Paulo: Contexto, 2018.

VOSOUGHI, Soroush; ROY, D.; ARAL, Sinan. *The spread of true and false news online*. Science, v. 359, n. 6380, p. 1146-1151, 2018.

XAVIER, Fábio C. *O que é o Projeto de Lei das Fake News e como isso pode impactar sua vida?* Security Leaders, 2024. Disponível em: https://securityleaders.com.br/o-que-e-o-projeto-de-lei-das-fake-news-e-como-isso-pode-impactar-sua-vida/. Acesso em: 17 abr 2024.

WAKEFIELD, Jane. Brittany Kaiser calls for Facebook political ad ban at Web Summit. *BBC News*. 06 nov. 2019. Disponível em: https://www.bbc.com/news/technology-50234144. Acesso em: 10 ago. 2022.

WALTER, Yoshija. Building human systems of trust in an accelerating digital and ai-driven world. *Frontiers in Human Dynamics*, 14 jun 2022. Disponível em: https://www.frontiersin.org/articles/10.3389/fhumd.2022.926281/full. Acesso em: 7 mai. 2023.

WARDLE, Claire. *Fake news. It's complicated*. First Draft News, 2017.

WARDLE, Claire.; DERAKHSHAN, H. Information disorder: Toward a new taxonomy framework for research and policy making. *Journal of International Affairs*, 2017.

WEBB, Michael; DOWLING, Melissa-Ellen; FARINA, Matteo. *Understanding Mass Influence: Three case studies of contemporary mass influence activities*. New South Wales: University of New South Wales, Aug 2021. 49 p.

WENLING, Duan; JIALI, Liu. 社交媒体战场上的认知对抗 *(trad. Guerra Cognitiva no Campo de Batalha das Redes Sociais)*. Jornal do Exército de Libertação. Ministério da Defesa Nacional da China, 02 fev 2023 Disponível em: http://www.mod.gov.cn/gfbw/jmsd/4931739.html. Acesso em: 09 jul. 2023.

WILSON III, Isaiah; SMITSON, Scott A. *The Compound Security Dilemma: Threats at the Nexus of War and Peace.* Parameters, Carlisle, v. 50, n. 2, p. 5-20, Summer 2020. Disponível em: https://ssi.armywarcollege.edu/wp-content/uploads/2020/05/Parameters_50-2_Summer-2020_Wilson.pdf. Acesso em: 25 jun. 2023.

YIN, Robert K. *Estudo de Caso: Planejamento e Métodos*. 2ª ed. Porto Alegre: Bookman, 2001.

YOSHIHARA, Toshi. *Chinese Information Warfare: A Phantom Menace or Emerging Threat?* Filipinas: University Press of the Pacific, 2004.

ZAREIE, A.; SAKELLARIOU, I. *Minimizing the spread of misinformation in online social networks*: A survey. Semantic Scholar, 2023. Disponível em: https://www.semanticscholar.org/paper/Minimizing-the-spread-of-misinformation-in-online-A-Zareie-Sakellariou/c645c2f1a256f15c0aadd78df6cd25ab5e197cdc. Acesso em: 16 jun. 2024.

ZIMDARS, Melissa.; Mcleod, Kembrew. *Fake news: understanding media and misinformation in the digital age.* EUA: MIT Press, 2020.

ZHANG, Linda. *Como combater a campanha de desinformação da China em Taiwan*. EUA: Military Review, 2021.

ZHONGQIU, Yao. *Cinco Séculos de Transformações: Como a China e o Ocidente Chegaram ao Momento Atual*. Escola de Estudos Internacionais e Centro de Estudos Políticos Históricos da Universidade de Renmin da China, vol. 1, nº 1, p. 17-39, 2023.

GLOSSÁRIO

A

Algoritmo - Sequências lógicas e estruturadas de instruções matemáticas que são utilizadas para resolver problemas ou executar tarefas específicas de forma automatizada por computadores ou outros dispositivos.

Algoritmos de personalização - São sistemas complexos que utilizam técnicas de aprendizado de máquina e inteligência artificial para adaptar experiências e conteúdos às preferências individuais dos usuários.

Agentes virtuais - São indivíduos, empresas ou até mesmo organizações governamentais que usam as redes sociais como ferramenta estratégica para estabelecer relacionamentos, se comunicar e impulsionar seus objetivos, envolvendo os públicos com os quais se relacionam e, até mesmo, moldando comportamentos.

B

***Big Data* -** Conjunto de dados grandes e complexos que não podem ser facilmente gerenciados ou analisados por métodos tradicionais de processamento de dados.

Bolhas de filtro - Fenômeno onde algoritmos e mecanismos de personalização, especialmente em plataformas digitais e redes sociais, limitam a exposição dos usuários a informações e perspectivas fora de suas preferências e comportamentos prévios.

Bolhas sociais - Grupos ou comunidades virtuais que são expostas e compartilham informações, opiniões e conteúdos que confirmam suas crenças e pontos de vista, criando um ponto de vista homogêneo.

***Bots* -** Programas de computador automatizados projetados para executar tarefas repetitivas e rotineiras de forma autônoma na internet.

C

***Click bait* -** Técnica que usa o exagero ou informações distorcidas para atrair a atenção e incentivar os usuários de internet a clicarem em um link ou acessar um conteúdo online.

Cognição - Processos mentais envolvidos na aquisição, processamento, armazenamento e utilização de informações.

D

***Dark Interations* -** Interação entre usuários de ambientes online, especialmente nas redes sociais, de uma maneira prejudicial ou indesejável.

***Deep Learning* -** Ou algoritmos de aprendizado profundo, são uma subcategoria de algoritmos de aprendizado de máquina (*machine learning*) desenvolvidos para realizar tarefas de aprendizado e reconhecimento de padrões.

***Deepfake* -** Tecnologia avançada de criação de conteúdo digital manipulado que utiliza aprendizado de máquina e inteligência artificial para alterar de forma realista imagens, áudios e vídeos.

Democracia - Sistema político que se caracteriza pela participação ativa dos cidadãos na vida política, com respeito aos direitos fundamentais e à igualdade perante a lei, visando evitar abusos de poder e autoritarismo, e garantindo soberania popular e proteção dos direitos e liberdades individuais.

Desinformação (*Disinformation*) - É a disseminação deliberada e intencional de informações falsas com o objetivo de enganar, manipular ou influenciar a opinião pública.

Desinformação de aluguel - Prática de pagar ou contratar terceiros para criar e disseminar informações falsas ou enganosas com o objetivo de influenciar a opinião pública, debates políticos ou processos eleitorais.

Dissonância cognitiva - Conceito psicológico introduzido por Leon Festinger em 1957. Estado psicológico de desconforto ou tensão mental que ocorre quando um indivíduo enfrenta informações ou comportamentos que são inconsistentes com suas crenças, valores ou atitudes preexistentes.

Domínio operacional - refere-se aos ambientes distintos em que as forças militares realizam operações para alcançar objetivos estratégicos. Cada domínio operacional possui características e desafios próprios, e as operações militares são adaptadas de acordo com as especificidades de cada um. Os principais domínios operacionais são: terrestre, marítimo, aéreo, espacial, cibernético e cognitivo.

E

***EdgeRank* -** Desenvolvido em 2009, foi um dos primeiros algoritmos a influenciar significativamente a forma como o conteúdo era apresentado aos usuários no Facebook, moldando a experiência das pessoas na plataforma, sendo, posteriormente, substituído por algoritmos mais avançados.

E-mails de *phishing* - Mensagens fraudulentas enviadas por criminosos cibernéticos com o objetivo de enganar os destinatários para que forneçam informações sensíveis, como senhas, números de cartão de crédito, ou outras informações pessoais.

Estado Democrático de Direito - Sistema em que o exercício do poder do Estado é limitado por normas jurídicas gerais que refletem a vontade geral da população. Ele busca impedir abusos de poder e garantir que os direitos fundamentais sejam respeitados, sendo a soberania popular um elemento central nessa estrutura.

Expressão Psicossocial - É a manifestação predominante de natureza psicológica e social dos recursos e indivíduos disponíveis na Nação. Compreende a interação de pessoas, ambiente e instituições sociais, com o objetivo de alcançar a satisfação e desenvolvimento da sociedade, promovendo a plena realização dos cidadãos e contribuindo para os Objetivos Nacionais.

F

Falsas verdades - Informações falsas apresentadas como verdadeiras com o objetivo de manipular a opinião pública, influenciar decisões ou causar algum tipo de dano.

***False Flag Attacks* -** São ações executadas com a intenção de iludir os observadores, fazendo com que pareçam ter sido realizadas por um grupo ou nação diferente do real responsável. Essas operações buscam desviar a atenção e a culpa do verdadeiro autor por meio de técnicas elaboradas.

Fake News - Notícias falsas ou informações deliberadamente enganosas, frequentemente disseminadas nas plataformas digitais e redes sociais, com o objetivo de manipular opiniões e enganar o público. Esses conteúdos são elaborados com técnicas e padrões de escrita jornalística para sejam percebidos como autênticos e confiáveis.

G

Guerra assimétrica - Forma de conflito caracterizada pelo uso de força militar organizada e prolongada. onde as partes envolvidas têm capacidades, estratégias e recursos desiguais.

Guerra cognitiva - Uso estratégico de informações, narrativas e influência psicológica para moldar percepções, opiniões e comportamentos de indivíduos e grupos, visando alcançar objetivos políticos, militares ou sociais.

Guerra de informação - São estratégias, táticas e ações utilizadas para influenciar, manipular, degradar ou interromper qualquer informação ou comunicação do oponente para alcançar ou garantir qualquer vitória ou objetivo necessário, seja política, social, militar ou econômica.

Guerra híbrida - Abordagem de conflito que combina vários métodos e táticas militares e não-militares de forma integrada.

H

Hipermobilidade estética - Capacidade dos usuários da internet de manipular, adaptar e transformar suas representações visuais e identidades digitais, o que inclui a criação, alteração e compartilhamento de imagens, avatares e perfis em diferentes plataformas digitais, ajustando a estética e a aparência conforme as tendências e preferências pessoais ou sociais.

I

Inteligência artificial generativa - Subcategoria da inteligência artificial que se refere a modelos de IA capazes de gerar novos conteúdos, como texto, imagens, áudio e vídeo, de forma autônoma, a partir de padrões aprendidos em dados de treinamento.

Infodemia - Epidemia de informações: termo criado em analogia à disseminação viral de agentes patógenos.

Inteligência artificial - Campo da ciência da computação que se concentra na criação de sistemas capazes de executar funções avançadas que normalmente requerem inteligência humana, incluindo a capacidade de ver, entender e traduzir idiomas falados e escritos, analisar dados, fazer recomendações etc. Também pode ser compreendida como um sistema computacional inteligente que possui capacidades cognitivas semelhantes às humanas, permitindo-lhe executar tarefas complexas de forma autônoma.

L

Literacia digital - Capacidade dos indivíduos de utilizar as tecnologias de forma crítica e eficaz, contribuindo para uma sociedade mais informada e participativa.

M

Má informação *(Malinformation)* - São informações verdadeiras, mas que são divulgadas com o intuito malicioso de causar dano, prejudicar a reputação de alguém ou desinformar deliberadamente.

Métodos convencionais de Defesa - Referem-se às estratégias, táticas e tecnologias tradicionais utilizadas pelas forças militares e de segurança para proteger um país, uma região ou ativos específicos.

***Microtargeting* -** Técnica de marketing e publicidade digital que envolve a segmentação e personalização de conteúdo e anúncios com base em dados detalhados sobre indivíduos ou pequenos grupos-alvo.

Misinformação (Misinformation) - Refere-se a informações falsas ou imprecisas que são divulgadas sem a intenção explícita de causar dano. Pode ocorrer devido a erros, má interpretação dos fatos ou falta de verificação.

Multidomínio - Um ambiente multidomínio é aquele onde operações e atividades são integradas e coordenadas por meio de vários, incluindo terra, mar, ar, espaço, ciberespaço e cognitivo, para alcançar objetivos estratégicos e táticos de forma eficaz e eficiente.

N

Névoa da guerra - Refere-se à incerteza, à confusão e à falta de informações claras que permeiam os cenários do conflito bélico.

Névoa digital - Em uma analogia à névoa da guerra, se caracteriza pela incerteza, confusão e falta de informações claras no ambiente digital.

O

Objetivos Nacionais - São metas estabelecidas por um país para orientar seu desenvolvimento econômico, social, cultural e de segurança, visando o bem-estar e progresso da Nação.

R

Realidade - Estado das coisas tal como elas realmente são, independentemente das percepções, crenças ou desejos individuais.

S

Segurança - Condição que permite ao país preservar sua soberania e integridade territorial, promover seus interesses nacionais, livre de pressões e ameaças, e garantir aos cidadãos o exercício de seus direitos e deveres constitucionais.

Soberania - Autoridade superior, indivisível e perpétua, que não admite limitações de ordem jurídica. Possui tanto uma dimensão interna, relacionada à garantia da segurança e harmonia social, quanto uma dimensão externa, referente à independência e não sujeição do país a qualquer poder estrangeiro ou organização internacional.

T

Teatro de operações - Área de conflito onde ocorrem operações militares.

Trolls -Usuários humanos ou *bots* que postam comentários, mensagens ou conteúdo com a intenção de provocar, irritar ou causar conflito entre as pessoas, muitas vezes de maneira intencional e maliciosa.

Tropas cibernéticas - Grupo de pessoas com objetivos unificados que usam a tecnologia de internet para conduzir operações cibernéticas.

V

Verdade - Informação que passou por processos rigorosos de verificação e que reflete de maneira precisa e confiável a realidade dos fatos.