Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

Artigo de pesquisa

Guilherme Dieguez Candido[1]
ORCiD 0009-0008-8770-7610

Mateus Flach Romani[2]
ORCiD 0009-0006-6481-8495

João Souza Neto[3]
ORCiD 0000-0002-4853-8788

A EXPLORAÇÃO DE FATORES HUMANOS E TECNOLÓGICOS EM CAMPANHAS DE DESINFORMAÇÃO PATROCINADAS POR ESTADOS-NAÇÕES

https://doi.org/10.58960/rbi.2025.20.287

Candido, Guilherme Dieguez, Mateus Flach Romani e João Souza Neto. 2025. "A exploração de fatores humanos e tecnológicos em campanhas de desinformação patrocinadas por Estados-nações," *Revista Brasileira de Inteligência* (ABIN) 20: e2025.20.287. https://doi.org/10.58960/rbi.2025.20.287.

Recebido em 11/08/2025
Aprovado em 20/10/2025
Publicado em 21/10/2025

1 Bacharel em Engenharia Civil pela Universidade Estadual de Maringá (UEM). Especialista em Ethical Hacking (VINCIT). Discente do programa de mestrado profissional em Segurança Cibernética (PPEE-UnB).

2 Bacharel em Engenharia de Produção pela Universidade de Brasília. Discente do programa de mestrado profissional em Segurança Cibernética (PPEE - UnB). Atua como pesquisador na área de Internet das Coisas - IoT.

3 Doutor em Engenharia Elétrica (UnB), Mestre em Engenharia Eletrônica pelo Instituto Internacional Philips na Holanda. É Pesquisador Associado no programa de Mestrado em Cibersegurança da Universidade de Brasília

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

A EXPLORAÇÃO DE FATORES HUMANOS E TECNOLÓGICOS EM CAMPANHAS DE DESINFORMAÇÃO PATROCINADAS POR ESTADOS-NAÇÕES

RESUMO

O objetivo deste artigo é conduzir uma revisão sistemática da literatura para investigar como atores estrangeiros empregam a desinformação como instrumento de interferência externa. A análise revela que ameaças exploram vulnerabilidades e limitações cognitivas humanas, manipulando vieses emocionais durante períodos de crise para distorcer a percepção da realidade. As mídias sociais e a Inteligência Artificial ocupam posição central nessas operações, viabilizando a amplificação através de bots sofisticados e deep fakes cada vez mais realistas. Uma resposta efetiva demanda a integração de medidas regulatórias, tecnológicas e sociais, incluindo fortalecimento de marcos legais, alfabetização midiática, monitoramento proativo e parcerias entre governo e sociedade civil. O estudo conclui que fortalecer a governança da informação constitui questão estratégica de soberania nacional e preservação democrática.

Palavras-chave: Desinformação, interferência externa, segurança cibernética, mídias sociais, inteligência artificial.

THE EXPLOITATION OF HUMAN AND TECHNOLOGICAL FACTORS IN STATE-SPONSORED DISINFORMATION CAMPAIGNS FOR FOREIGN INTERFERENCE PURPOSES

ABSTRACT

The aim of this article is to conduct a systematic literature review to investigate how foreign actors employ disinformation as an instrument of external interference. The analysis reveals that threats exploit human vulnerabilities and cognitive limitations, manipulating emotional biases during periods of crisis to distort the perception of reality. Social media and Artificial Intelligence occupy a central position in these operations, enabling amplification through sophisticated bots and increasingly realistic deepfakes. An effective response demands the integration of regulatory, technological, and social measures, including strengthening legal frameworks, media literacy, proactive monitoring, and partnerships between government and civil society. The study concludes that strengthening information governance constitutes a strategic issue of national sovereignty and democratic preservation.

Keywords: *Disinformation, foreign interference, cybersecurity, social media, artificial intelligence.*

LA EXPLOTACIÓN DE FACTORES HUMANOS Y TECNOLÓGICOS EN CAMPAÑAS DE DESINFORMACIÓN PATROCINADAS POR ESTADOS-NACIÓN

RESUMEN

El objetivo de este artículo es realizar una revisión sistemática de la literatura para investigar cómo los actores extranjeros emplean la desinformación como instrumento de interferencia externa. El análisis revela que amenazas explotan vulnerabilidades y limitaciones cognitivas humanas, manipulando sesgos emocionales durante períodos de crisis para distorsionar la percepción de la realidad. Las redes sociales y la Inteligencia Artificial ocupan una posición central en estas operaciones, posibilitando la amplificación através de bots sofisticados y deepfakes cada vez más realistas. Una respuesta efectiva demanda la integración de medidas regulatorias, tecnológicas y sociales, incluyendo marcos legales fortalecidos, alfabetización mediática y alianzas entre gobierno y sociedad civil. El estudio concluye que fortalecer la gobernanza de la información constituye una cuestión estratégica de soberanía nacional.

Palabras clave: Desinformación, interferencia externa, seguridad cibernética, redes sociales, inteligencia artificial.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

Introdução

À medida que as revoluções da informação transformam a sociedade global, elas naturalmente abrem novos espaços para contestação e conflito (Whyte 2020a). Como afirma a Política Nacional de Inteligência do Brasil - PNI, de 2016:

> A conjuntura mundial tem alterado a percepção e a conduta dos Estados nacionais, das organizações e dos indivíduos, realçando os chamados temas globais e transnacionais. [...] As relações internacionais não se resumem ao exame de temas de convergência e a ações cooperativas [...]. O ambiente internacional caracteriza-se, ao contrário, pela contínua competição entre Estados. Cada um busca melhorar seu respectivo posicionamento estratégico (BRASIL 2016).

A era digital mudou permanentemente a forma como os Estados conduzem a guerra política, exigindo um reequilíbrio das prioridades de segurança nas democracias. A utilização do ciberespaço por atores estatais e não-estatais para subverter eleições democráticas, incentivar a proliferação da violência e desafiar a soberania e os valores dos Estados têm gerado um efeito altamente desestabilizador (Paterson e Hanley 2020). Dependendo do contexto e dos alvos, as consequências podem assumir diversas formas, incluindo o fomento à radicalização e ao recrutamento por grupos extremistas violentos. A intensificação do discurso de ódio em contextos de fragilidade polariza comunidades sociais e políticas (Duarte 2024).

Nas últimas décadas, a proliferação de *fake news* e campanhas de desinformação destinadas a manipular a opinião pública tem sido particularmente intensa durante períodos eleitorais e momentos de conflito militar (López-Cantos 2024). Estados podem aumentar as tensões geopolíticas criando notícias falsas, disseminando boatos ou forjando apoio a agendas próprias (Lapke e Browning 2024). Adversários estrangeiros usam desinformação para promover discursos alinhados aos seus interesses, o que geralmente envolve a disseminação de narrativas falsas que favorecem a nação estrangeira enquanto minam a coesão social e os objetivos políticos da nação-alvo (Vasist e Krishnan 2024). Nações se engajam em conflitos informacionais usando dados frequentemente falsos para obter vantagem sobre adversários. Muitas delas conduzem campanhas encobertas de desinformação no exterior, o que configura interferência externa (Işık *et al*. 2022).

Dentro desse contexto, torna-se cada dia mais evidente a importância do debate sobre campanhas de desinformação patrocinadas ou perpetradas por Estados-nações, incluindo suas especificidades técnicas, especialmente

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

àqueles que lidam com o processo decisório nacional ou seu assessoramento. Compreender como fontes externas de ameaça têm agido no ambiente cibernético para explorar fatores humanos e tecnológicos a fim de interferir na opinião pública nacional é essencial para que o Estado possa traçar estratégias eficazes de prevenção, detecção, obstrução e neutralização destas ações adversas.

Assim, a presente pesquisa teve como principal objetivo mapear, organizar e descrever o conhecimento existente sobre campanhas de desinformação digital patrocinadas por Estados-nações, a fim de auxiliar em práticas de segurança, políticas públicas e melhorias tecnológicas, processuais ou de intervenção que visem seu enfrentamento. Ademais, tem caráter utilitário, direcionado a melhorias tecnológicas, processos ou intervenções em contextos reais.

A abordagem é qualitativa, uma vez que se baseia na interpretação e análise de textos acadêmicos para compreender as táticas, os fatores humanos explorados e o papel das tecnologias em campanhas de desinformação. Possui ainda caráter exploratório e descritivo, pois busca mapear, sistematizar e descrever o conhecimento existente sobre o assunto. O procedimento técnico adotado foi a revisão bibliográfica sistemática, com busca estruturada e critérios de inclusão e exclusão definidos para garantir rigor e reprodutibilidade, que buscou responder às seguintes questões:

1. Como atores estrangeiros exploram fatores humanos para aumentar a eficácia de operações de desinformação digital?
2. Qual o papel das mídias sociais e da Inteligência Artificial nas operações de desinformação para fins de interferência externa?
3. Como táticas centradas no ser humano podem ser modeladas para dar suporte à detecção de ameaças em campanhas de desinformação digital?

Para garantir uma revisão abrangente e reprodutível, adotou-se uma abordagem de busca sistemática baseada em diretrizes estabelecidas para síntese de literatura. A busca foi realizada na base *Scopus*. As consultas de busca foram construídas utilizando combinações de palavras-chave relevantes e operadores booleanos. Exemplos de termos de busca primários incluem: "*disinformation*", "*state sponsored*", "*foreign influence*" e "*foreign interference*". A busca inicial foi limitada a publicações realizadas entre 2020 e 2025; a áreas das Ciências Sociais, Ciência da Computação, Engenharia e Psicologia; e a artigos de periódicos e de conferências, revisados por pares e publicados em língua inglesa.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

Todos os registros recuperados foram importados para uma ferramenta de gerenciamento de referências e passaram por deduplicação. Títulos e resumos foram analisados de forma independente por dois revisores, com eventuais divergências resolvidas por consenso. Os textos completos dos artigos restantes foram então avaliados com base em critérios de inclusão pré-definidos.

Os critérios de inclusão foram: (1) Estudos que abordem campanhas de desinformação patrocinadas por Estados ou atores estrangeiros; (2) Estudos que investiguem operações de influência ou interferência externa; (3) Trabalhos que analisem o uso de fatores humanos em campanhas de desinformação; e (4) Estudos que discutam o papel das mídias sociais, inteligência artificial ou outras tecnologias digitais em operações de desinformação.

Por sua vez, os critérios de exclusão foram: (1) Estudos que tratavam de estudos de caso ou de países específicos; e (2) Artigos que possuíam acesso restrito. Ao final, foram analisados 29 artigos que atenderam aos critérios de pesquisa. Para avaliar sistematicamente a literatura, dados estruturados foram extraídos de cada artigo selecionado e sintetizados com base nas perguntas de pesquisa.

A exploração de fatores humanos na eficácia de operações de desinformação digital

O termo ciberespaço é geralmente utilizado em referência às interações realizadas por meio da rede mundial de computadores (Paterson e Hanley 2020). Os conflitos informacionais têm sido, até agora, geralmente compreendidos em termos da superfície de ataque dos sistemas de informação e comunicação habilitados em rede (Whyte 2020b). Contudo:

> Os prejuízos das ações no espaço cibernético não advêm apenas do comprometimento de recursos da tecnologia da informação e comunicações. Decorrem, também, da manipulação de opiniões, mediante ações de propaganda e desinformação (BRASIL 2016).

A desinformação e o controle da informação são aspectos fundamentais a serem examinados ao se atribuir o uso intencional de um ataque cibernético com o objetivo de influenciar a opinião pública doméstica sobre um líder ou política de Estado, ou de moldar a percepção internacional sobre determinada questão (Lapke e Browning 2024). O conceito de desinformação é contextualmente relacionado ao de pós-verdade. ‘‘Pós-verdade’’ é um termo que se refere a circunstâncias em que fatos objetivos são menos influentes na formação da opinião pública do que apelos à emoção e crenças pessoais. É conceitualmen-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

te amplo o suficiente para englobar muitas expressões, incluindo *fake news*, informação errônea (*misinformation*) e desinformação (*disinformation*). Um elemento-chave que pode diferenciar estes termos é a intenção (Wu 2023). Informação errônea refere-se a informações incorretas divulgadas de forma não intencional, enquanto a desinformação é composta por informações falsas criadas intencionalmente com o propósito de enganar outras pessoas (Smith 2021). Entretanto, estes conceitos estão profundamente entrelaçados, já que pode ser difícil identificar a natureza da intenção da fonte (García Santamaría *et al*. 2024). Segundo a Doutrina da Atividade de Inteligência:

> A desinformação é o conjunto de ações que dissemina deliberadamente informações falsas, com o intuito de enganar ou confundir público-alvo específico para causar dano, induzir ao erro ou manipular situação ou evento em prol dos interesses do patrocinador. [...] Para ser mais eficaz, a desinformação deve conter elementos de veracidade ou plausibilidade em seu conteúdo (ABIN 2023, 73).

Há uma infinidade de formas pelas quais a desinformação é utilizada nas relações internacionais. Atores estrangeiros utilizam estrategicamente a manipulação emocional, os vieses cognitivos e culturais, as redes de confiança e as limitações do julgamento humano e das máquinas para aumentar a eficácia de seus esforços (Saeidnia *et al*. 2025). Quando orquestrada por Estados ou organizações, especialmente contra outros países, a desinformação se enquadra na guerra informacional (Kumar *et al*. 2025), transformando-se, assim, em uma ferramenta utilizada na disputa de poder em escala global (la Cour 2020).

A desinformação estrangeira opera em uma escala diferente das iniciativas domésticas, representando uma questão entre Estados, com potencial para escalar em disputas diplomáticas ou até mesmo em conflitos armados. Estados que conduzem campanhas de desinformação transfronteiriças geralmente dispõem de orçamentos muito maiores do que os veículos de mídia de países pequenos ou médios, o que evidencia o caráter assimétrico deste tipo de conflito. As campanhas podem fazer parte de estratégias voltadas à desestabilização de outras nações e à criação de condições para uma escalada posterior (Wagnsson *et al*. 2025).

O uso da desinformação para desgastar instituições democráticas tem sido um método amplamente adotado por Estados, pois apresenta custos de implementação relativamente baixos e gera resultados quase imediatos e de difícil reversão. Ataques de desinformação são voltados a corroer a confiança dos cidadãos na autoridade legítima ou no próprio sistema democrático (Ivan *et al*. 2021). Do ponto de vista financeiro, as ameaças cibernéticas baseadas

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

em desinformação representam uma opção atraente para os interesses estratégicos estatais, já que direcionar centenas de *bots* online custa apenas uma fração do que seria gasto com outras opções de defesa ou espionagem (Lapke e Browning 2024).

Uma das características dos conflitos humanos é o desejo de influenciar o processo decisório do adversário e forçá-lo a tomar decisões previamente determinadas pelo lado que exerce a interferência. Isso pode ser alcançado por meio do envio de informações especialmente selecionadas (Ivan *et al*. 2021).

Ataques cibernéticos de desinformação podem infligir danos psicológicos profundos às comunidades, explorando vulnerabilidades humanas (Katagiri 2023). Campanhas exploram emoções e vieses cognitivos - usam artifícios emocionais e retóricos para levar as pessoas a compartilharem e acreditarem em conteúdo falso, muitas vezes convencendo indivíduos a agir contra seus próprios interesses ao semear confusão e desconfiança (Işık *et al*. 2021 2022). Para a ABIN, em sua Doutrina da Atividade de Inteligência (2023), ‘‘adicionalmente às incertezas derivadas dos limites cognitivos, a própria forma como a realidade se apresenta ao ser humano pode ser ofuscada pela desinformação’’. Especialmente quando empregada por atores estrangeiros hostis, a desinformação é criada e disseminada intencionalmente com o propósito de enganar e manipular a opinião pública (Cartwright *et al*. 2022).

Em seu trabalho, Smith (2021) afirma que atores cibernéticos maliciosos estão manipulando o público em períodos de tensões globais, quando os indivíduos estão mais suscetíveis à desinformação. Em 2020, a Organização Mundial da Saúde (OMS) anunciou que o Corona vírus estava acompanhado por uma ‘‘infodemia’’ - uma superabundância de informações (algumas precisas e outras não) o que dificultava que as pessoas encontrassem fontes confiáveis e orientações seguras. A infodemia é um fenômeno que tem alimentado a propagação de ameaças cibernéticas por atores que se aproveitam justamente da confusão provocada por determinados eventos para disseminar informações falsas ao público em geral. Isso resulta na erosão da segurança, da dignidade humana e da equidade no ciberespaço. Eventos trágicos em escala global evocam respostas emocionais e atores maliciosos se aproveitam dessa característica humana.

No mesmo sentido, Duarte (2024) nota que campanhas de desinformação vinculadas a crises emergenciais oferecem condições propícias para operações de interferência contra comunidades, pois é justamente quando elas estão mais vulneráveis. Atualmente, esse tipo de ação é facilitado pelo amplo acesso

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

à Internet e pela proliferação dos meios de comunicação, que se tornaram o meio mais eficaz para transmitir ideologias e ideias. São atividades orientadas por narrativas, utilizando palavras, imagens e ações sincronizadas. Essas campanhas dependem mais do canal que difunde a informação do que da natureza da própria informação. García Santamaría *et al*. (2024) corroboram ressaltando que informações falsas ou enganosas podem ser consideradas críveis se forem percebidas como autênticas e replicadas por redes confiáveis.

Wu (2023) adiciona que a "diplomacia pública da pós-verdade" é uma nova forma de diplomacia pública, que emprega conteúdo gerado por meio de redes sociais, supervisionada por países para interferir nas condições cognitivas e afetivas de públicos em países-alvo. Tem sido praticada principalmente por meio de canais de comunicação na Internet e em dispositivos móveis, transcendendo as fronteiras nacionais.

Smith (2021) destaca que meios de comunicação versáteis dificultam os procedimentos de verificação de fatos (*fact checking*), que não conseguem acompanhar a velocidade com que as informações circulam na Internet. Isso oferece aos cibercriminosos uma flexibilidade ainda maior para espalhar informações falsas que apelam às emoções humanas, por meio de mensagens que transmitem senso de urgência ou imitam figuras de autoridade.

La Cour (2020) constata que aplicar uma abordagem emocional à desinformação é particularmente frutífero, pois a desinformação frequentemente aparece em combinação com discursos de ódio e apelos a emoções como raiva, ressentimento e medo. Watney (2023) acrescenta que mensagens enganosas utilizam imagens ou vídeos fora de contexto, reaproveitados unicamente para alarmar e aprofundar o senso de pânico e ansiedade.

Para Whyte (2020a), operações cibernéticas frequentemente resultam em efeitos sociopsicológicos no nível da população nacional. Tanto os incidentes cibernéticos quanto a imagem de vulnerabilidade generalizada que eles promovem contribuem para um mal-estar informacional popular, em que a confiança pública na origem e na qualidade das informações transmitidas por comentaristas, especialistas e até mesmo por outros cidadãos diminui.

Operações cibernéticas disruptivas são frequentemente um elemento crucial para impedir que vozes democráticas proeminentes assumam um papel direto no combate à desinformação. Para o público em geral, o simples conhecimento de uma interferência externa, ainda que inespecífica, pode reduzir a confiança em atores-chave e instituições relevantes. Ataques cibernéticos

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

são frequentemente direcionados a alvos políticos ou instituições públicas de valor simbólico. Cidadãos que presenciam ataques a alvos de importância nacional costumam interpretar que as ameaças estrangeiras estão sendo dirigidas contra a infraestrutura convencional, em vez da, geralmente mais difícil de conceber, funcionalidade democrática.

Ivan *et al*. (2021) contribuem dizendo que as campanhas de desinformação têm sido usadas no campo social para explorar as oportunidades proporcionadas pelas tecnologias digitais com o objetivo de alcançar fins manipulativos em torno de temas controversos. Estas campanhas estão sendo amplamente utilizadas - às vezes em combinação com outros ataques cibernéticos - por uma variedade de atores domésticos e estrangeiros para semear desconfiança e criar polarização social. Ataques de desinformação têm como objetivo a erosão da confiança dos cidadãos na autoridade legítima ou no próprio sistema democrático, minando os valores culturais compartilhados.

Por fim, Wagnsson *et al*. (2025) afirmam que a necessidade das pessoas se tornarem mais críticas em relação às informações que encontram online baseia-se no que pode ser chamado de teoria da ‘‘verdade padrão’’ (*truth-default theory*), que sugere que os seres humanos são naturalmente inclinados a acreditar nos outros e a presumir que a comunicação é honesta, a menos que existam sinais claros de engano.

O papel das mídias sociais e da Inteligência Artificial nas operações de desinformação para fins de interferência externa

A Estratégia Nacional de Inteligência do Brasil - ENINT, de 2017, define interferência externa como sendo:

> A atuação deliberada de governos, grupos de interesse, pessoas físicas ou jurídicas que possam influenciar os rumos políticos do País com o objetivo de favorecer interesses estrangeiros em detrimento dos nacionais (BRASIL 2017, 17).

Em síntese, a influência e a interferência estrangeiras envolvem esforços encobertos de uma nação para moldar ou desestabilizar os assuntos de outra (Kumar *et al*. 2025). Ao analisar o que muitos têm chamado, nos últimos anos, de ‘‘hackeamento de eleições’’, ‘‘interferência eleitoral’’ e ‘‘ingerência estrangeira’’, estudiosos frequentemente recorrem ao uso de rótulos como ‘‘guerra híbrida’’. De forma ampla, esses termos descrevem o uso de diversos elementos do arsenal estatal de interferência externa a serviço de objetivos estratégicos (Whyte 2020a).

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

Por sua vez, a Doutrina da Atividade de Inteligência da Agência Brasileira de Inteligência - ABIN, de 2023, conceitua e explica a interferência externa da seguinte forma:

> É uma forma encoberta de projetar poder, tratando-se de um instrumento para influenciar o outro a modificar seu comportamento conforme os interesses do patrocinador da ação. Seu caráter velado serve para moldar os acontecimentos em prol do patrocinador, que precisa se manter oculto como pressuposto para alcançar os resultados desejados (ABIN, 2023).

As ações de interferência externa possuem objetivos estratégicos definidos, que geralmente se concentram no campo político-social ou econômico. No primeiro, entre os diversos objetivos possíveis, a ação pode procurar influenciar diretamente o processo decisório; buscar distrair ou manipular um público específico; minar o capital político e social do adversário; apoiar grupos internos para mudanças de políticas públicas; ou, no extremo, mudar o regime político de outro Estado. No campo econômico, alguns dos objetivos frequentes são prejudicar concorrentes; cercear desenvolvimento tecnológico, econômico ou comercial; estimular boicotes; e desestabilizar mercados (ABIN 2023, 72-73).

Como ressaltado pela PNI (2016), ações que atentem contra a autodeterminação, a não-ingerência nos assuntos internos e o respeito incondicional à Constituição e às leis são classificadas como ações contra a soberania nacional. Desta forma:

> É prejudicial à sociedade brasileira que ocorra interferência externa no processo decisório ou que autoridades brasileiras sejam levadas a atuar contra os interesses nacionais e em favor de objetivos externos antagônicos. A interferência externa é uma ameaça frontal ao princípio constitucional da soberania (BRASIL 2016).

Para a ABIN (2023), "o potencial nocivo de notícias enganosas acompanha o crescimento exponencial da massificação informacional e da sofisticação tecnológica dos recursos digitais, cada vez mais baratos e acessíveis". Para Ambros (2024):

> "Novas tecnologias, [...], como as redes sociais, a Inteligência Artificial e maiores capacidades de coleta e processamento de dados, aumentaram significativamente a sofisticação e a velocidade na exploração do domínio informacional, ao mesmo tempo que diminuíram seus custos" (Ambros 2024, 4).

A disseminação de desinformação como ameaça cibernética é frequentemente realizada por meio da exploração de plataformas de mídia social. Com essas plataformas tendo experimentado um crescimento acentuado tanto no

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

número de usuários quanto no engajamento diário ao longo da última década, utilizar as redes sociais para popularizar uma narrativa ou impulsionar o engajamento em torno de um tema de interesse estatal tornou-se relativamente fácil (Lapke e Browning 2024). Operações frequentemente combinam desinformação com outros ataques cibernéticos, vazamentos de dados e produção de conteúdo inautêntico nas redes sociais. A maioria das contribuições acadêmicas sobre as tendências da pós-verdade enfatiza o papel da Internet e da invenção de novas tecnologias de informação e comunicação como facilitadoras (la Cour 2020).

Os desenvolvimentos tecnológicos transformaram a ecologia midiática, levando a uma crise dos meios de comunicação tradicionais e dando origem a uma grande indústria de desinformação e ciência de baixa qualidade (la Cour 2020). Nas redes sociais, atores exploram e manipulam situações espalhando desinformação e incitando violência para promover suas próprias agendas (Watney 2023), transmitindo mensagens dissuasivas e enganosas que fomentam a confusão pública e a desconfiança em relação a instituições e à ciência (García Santamaría *et al*. 2024). Campanhas de desordem informacional conduzidas online por meio das redes sociais podem impactar de forma imediata dinâmicas políticas, geopolíticas e de segurança. A instrumentalização das mídias sociais é uma prática de fácil acesso para quase todos os atores (Duarte 2024).

Duarte (2024) destaca que a informação falsa se multiplica de forma rápida e barata por meio das plataformas de mídia social. O objetivo principal é moldar a percepção, criando divisões e interferindo em diferentes processos decisórios, com o propósito concreto de alterar dinâmicas sociais e políticas. Logo, para os perpetradores desse tipo de ação, é crucial inundar blogs e redes sociais com *fake news* e narrativas alternativas sobre eventos noticiosos, a fim de dificultar a capacidade da população de distinguir fato de ficção. Assim, a disseminação de narrativas falsas e/ou incitadoras, aliada à sua propagação sistemática por meio das plataformas de mídia social, pode culminar na interrupção, corrupção ou usurpação do processo decisório.

Como ressaltam DiResta *et al*. (2021), as mídias sociais são projetadas para permitir que qualquer pessoa com uma mensagem consiga direcioná-la de forma precisa ao público ideal. Essa capacidade está tão disponível para profissionais de marketing e ativistas políticos legítimos quanto para aqueles que realizam operações de interferência patrocinadas por Estados. Quando as campanhas de desinformação utilizam canais de mídia social, conseguem alcançar populações específicas com muito mais facilidade do que o fariam

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

em canais convencionais de transmissão. Desta forma, agentes de desinformação habilidosos podem personalizar narrativas para públicos específicos. Além disso, os recursos de compartilhamento garantem que publicações atraentes tenham potencial para se disseminar por meio de transmissões *peer-to-peer*, alcançando um público amplo e aumentando a confiança no conteúdo, já que ele é compartilhado por alguém conhecido do destinatário.

Conforme acrescenta Duarte (2024), o enredo se complica ainda mais quando se considera a propagação de "*deep fakes*" nas plataformas de mídia social. *Deep fakes* são simulações digitais de imagem e voz produzidas por meio de *deep learning* no campo da Inteligência Artificial. Esse recurso tecnológico é caracterizado por um alto poder de simulação e realismo. Por isso, é frequentemente utilizado com intenções maliciosas, tanto em crimes cibernéticos comuns quanto em campanhas de desinformação de cunho político e militar. São conteúdos de imagem, áudio ou vídeo editados de forma tão sofisticada que retratam de forma realística personalidades dizendo ou fazendo coisas que, na verdade, nunca disseram ou fizeram. Um deep fake disseminado no momento certo pode ser usado de forma eficaz para enganar eleitores e criar ou agravar tensões políticas, interferindo fortemente ou até mesmo alterando o resultado de eleições democráticas (Paterson e Hanley 2020).

Segundo Paterson e Hanley (2020), os avanços em Inteligência Artificial e aprendizado de máquina também permitem que contas automatizadas em redes sociais se tornem cada vez mais sofisticadas na imitação do comportamento humano. O uso das mídias sociais como parte de operações mais amplas de guerra informacional representa um grande desafio e que os progressos tecnológicos tendem a ampliá-lo ainda mais, trazendo abordagens e ferramentas variadas - como os *deep fakes* - que podem auxiliar na condução de campanhas de guerra política. Os Estados precisam ir além dos métodos tradicionais de coleta de inteligência para garantir que mensagens maliciosas não estejam influenciando negativamente seus cidadãos.

Historicamente, operações de desinformação conduzidas por governos eram realizadas por forças militares ou serviços de inteligência. Mais recentemente, campanhas descobertas em plataformas de mídia social incluem um número significativo de operações terceirizadas que são executadas por contratados ou por exércitos de cidadãos sem vínculo formal com o governo e forças armadas (DiResta *et al*. 2021). Usuários não apenas contribuem para o conteúdo de pós-verdade - seja por causa de seus próprios interesses e perspectivas pessoais ou em nome de outros agentes patrocinadores -, mas também atuam como amplificadores, dispostos e eficazes em gerar impacto direto em públi-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

cos de determinadas localidades ou dentro de redes específicas (Wu 2023).

DiResta et al. (2021) ressaltam ainda que os Estados que decidem conduzir operações de interferência encobertas precisam fazer uma escolha fundamental: planejar e implementar a operação internamente, terceirizar o trabalho para mercenários digitais ou adotar uma combinação dessas estratégias. Mercenários digitais oferecem vantagens significativas. Dão ao Estado acesso a profissionais altamente qualificados que podem gerar economia de recursos, tornar as campanhas mais furtivas e proporcionar negação plausível em caso de exposição. Ao terceirizar, o Estado pode aproveitar mais facilmente novas tecnologias e as práticas mais atuais de marketing digital em redes sociais, aumentando o alcance da campanha de desinformação. Isso inclui estratégias multiplataforma que exploram os recursos específicos de cada mídia social para maximizar a interferência almejada.

Megiddo (2020) relata que pesquisadores também identificaram milícias digitais voluntárias, amadoras ou profissionais, que podem ser remuneradas ou não. Utilizar milícias digitais ou *bots* é útil para ocultar a origem governamental da enxurrada de conteúdo e fazer com que ela pareça mais autêntica e distribuída, ao diversificar o perfil das contas que participam da disseminação da desinformação. Essa prática é conhecida como "*astroturfing*". Além do *astroturfing*, uma tática de abafamento é o "sequestro de *hashtag*", em que uma *hashtag* associada a determinado movimento político é apropriada por seus opositores, que passam a postar em grande escala mensagens contrárias à mensagem original, mas utilizando a mesma *hashtag*. Tanto o abafamento quanto a desinformação podem ser realizados de forma eficaz por meio do uso de *microtargeting*. Muitos sites hoje geram perfis extremamente detalhados dos usuários, o que facilita a veiculação de publicações para grupos-alvo muito específicos, como já mencionado anteriormente.

Para Whyte (2020b), a estratégia de interferência externa depende das ações de vozes significativas já estabelecidas dentro de comunidades de interesse. Às vezes, isso ocorre por meio de indivíduos recrutados. Entretanto, em outros casos, *trolls* utilizam plataformas de mídia social para tentar fazer com que seu conteúdo seja notado, personalizando seu comportamento para atrair alvos específicos. Em essência, trata-se de um *spear phishing* nas redes sociais, cujo objetivo é ser notado e amplificado por outros usuários com presença já consolidada.

Megiddo (2020) concorda dizendo que a amplificação de mensagens é realizada por meio de redes de contas humanas, reais ou falsas, com o apoio de

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

bots ou ferramentas que facilitam significativamente a capacidade de curtir, comentar e compartilhar a partir de várias contas ao mesmo tempo. *Bots*, em particular, têm sido usados para atacar ou silenciar críticos, aumentar o número de seguidores e amplificar as mensagens de candidatos políticos, além de disseminar propaganda e desinformação para manipular a opinião pública.

Atores estrangeiros frequentemente implementam redes de *bots* como tática contra países-alvo - por exemplo, para interferir em eleições, minar a confiança pública ou polarizar debates. Um desafio central para essas operações é justamente evitar a detecção pelas plataformas e pelos usuários do país-alvo. É o que dizem Kumar *et al*. (2025), explicando que campanhas eficazes de desinformação costumam depender de numerosos agentes de perfil discreto em vez de um único mega-influenciador. Numa campanha de interferência externa, o objetivo é espalhar uma narrativa de forma sutil, evitando que qualquer conta falsa se torne tão proeminente a ponto de levantar suspeitas.

Bots costumam se comportar como usuários reais. Como contas influentes de verdade postam com frequência, um bot também postará regularmente - mas apenas até o ponto em que isso não chame atenção. Quem segue ou vê essas postagens pode ser influenciado pelo conteúdo, acreditando que seja uma opinião humana genuína. A vida útil de um bot pode ser longa, mas ele nunca se torna um mega-influenciador. Isso implica que ele pode influenciar muitas pessoas ao longo do tempo, mas permanecendo sempre abaixo do limiar da notoriedade. Usuários humanos e algoritmos têm menos chance de identificar um bot que não está entre as contas mais populares, permitindo que ele continue operando e influenciando opiniões ou espalhando desinformação de forma discreta (Kumar *et al*. 2025).

Modelagem de táticas centradas no ser humano para detecção de ameaças em campanhas de desinformação digital

Conter a disseminação da desinformação e garantir uma infraestrutura cibernética segura deve ser uma prioridade nas agendas estatais (Smith 2021). É o que alerta a PNI (2016) ao mencionar que:

> Há países que buscam abertamente desenvolver capacidade de atuação na denominada guerra cibernética, ainda que os ataques dessa natureza possam ser conduzidos não apenas por órgãos governamentais, mas também por grupos e organizações criminosas; por simpatizantes de causas específicas; ou mesmo por nacionais que apoiem ações antagônicas aos interesses de seus países (BRASIL 2016).

Combater a desinformação envolve uma combinação de estratégias: fortale-

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

cer marcos legais contra interferência estrangeira, melhorar a alfabetização midiática e a conscientização pública, implementar ferramentas tecnológicas e promover a transparência nas fontes de informação (Işık *et al.* 2022). Se as operações de guerra informacional têm como objetivo alterar os contornos do ambiente informacional para convencer os cidadãos de que determinado discurso não é confiável ou é obra de "forças obscuras" na sociedade, então uma tarefa crítica para aqueles que buscam modelar a ameaça de forma mais eficaz é mapear o cultivo de narrativas e de temas que atingem tais objetivos (Whyte 2020b).

A redução da superfície de ataque das democracias deve, inevitavelmente, surgir em grande parte de parcerias entre a sociedade civil e o governo. Uma estratégia de dissuasão deve ser aplicada para moldar o comportamento de adversários estrangeiros de forma que seus esforços tenham pouca probabilidade de sucesso (Whyte 2020c). Educar os usuários para reconhecer sinais de desinformação ou de *bots* pode engajar o público na denúncia de contas suspeitas. A vigilância comunitária é uma camada de mitigação que complementa a detecção automatizada (Kumar *et al*. 2025).

Wagnsson *et al*. (2025) comentam que governos e outras organizações têm lançado diversas contramedidas para enfrentar o problema da desinformação disseminada por adversários estrangeiros. Uma forma de mitigar alguns dos efeitos negativos associados à desinformação é informar os cidadãos de que estão "sob ataque". Uma ameaça percebida à comunidade tende a estreitar a identificação com o grupo. Especificamente, a presença de uma ameaça externa à nação deve aumentar a saliência da identidade nacional dos cidadãos, ou seja, fazê-los identificar-se mais fortemente com seu pertencimento nacional. Esse senso fortalecido de coesão nacional deve aumentar as intenções pró-sociais e a confiança dentro do grupo, podendo inibir conflitos entre subgrupos com divisões políticas. A ideia de ativar a identidade nacional, portanto, não é fomentar o nacionalismo, mas sim reforçar o senso de coesão social, incentivando as pessoas a deixarem de lado suas diferenças e a confiarem umas nas outras diante de um desafio comum.

Para Smith (2021), a maneira mais eficaz de conter o avanço da infodemia é adotar uma abordagem centrada no ser humano e orientada por evidências, que busque responsabilizar os atores envolvidos. Esse caminho deve envolver ativamente as vítimas de ataques cibernéticos e o Estado. Também é necessário um esforço para organizar melhor o fluxo de informações e assegurar a existência de órgãos de verificação de fatos em número suficiente para combater a disseminação da desinformação no ciberespaço. Outra consideração

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

importante é a necessidade de garantir que as vítimas de ataques cibernéticos sejam ouvidas, a fim de compreender melhor a natureza desses ataques e seus impactos. As discussões devem ser orientadas para o custo humano da infodemia, resultado da exposição a informações falsas e do aumento da vulnerabilidade às ameaças cibernéticas.

Vasist e Krishnan (2024) afirmam que quando o público e as instituições governamentais se tornam mais conscientes sobre desinformação, torna-se mais difícil para falsidades maliciosas criarem raízes. Campanhas de conscientização, educação para alfabetização midiática e monitoramento proativo por agências de inteligência são ferramentas sugeridas nesse contexto. Uma maior preparação das agências permite identificar operações de desinformação mais rapidamente para neutralizá-las ou desmenti-las antes que se espalhem amplamente. Mecanismos de defesa robustos - desde o compartilhamento de inteligência sobre ameaças de desinformação até a proteção de canais de informação - continuam sendo vitais. Na prática, isso pode significar investir em cibersegurança, monitorar veículos de propaganda patrocinados por outros Estados e tornar públicas as tentativas de interferência externa.

Para Ivan et al. (2021), as sociedades democráticas precisam investir na construção de resiliência e resistência contra essa nova forma complexa de conflito, como por exemplo: (1) criar um sistema deliberativo que informe e mobilize os cidadãos, facilitando a transformação por meio da conscientização, do desenvolvimento de competências e do estímulo ao pensamento reflexivo e crítico; (2) aumentar a capacidade de cooperar no desenvolvimento de uma abordagem adaptativa e coletiva para a detecção de propaganda e desinformação; e (3) promover fluxos de cooperação entre atores governamentais, empresas digitais e de tecnologia, veículos de mídia e organizações da sociedade civil.

Wu (2023) destaca que muitos países já lançaram programas apoiados por inteligência artificial que podem automaticamente filtrar e identificar desinformação ou informação errônea na Internet. Alternativamente, novas leis e regulamentações sobre o funcionamento da mídia - em especial no que diz respeito a seus algoritmos e à proteção da privacidade - deveriam ser criadas para mitigar os impactos negativos gerados pela pós-verdade. A verificação sistemática e constante de fatos, bem como a detecção da "diplomacia pública da pós-verdade" por entidades independentes, sem fins lucrativos e apartidárias, deve ser uma necessidade para proteger o público em geral de ser enganado ou iludido. Treinamentos de alfabetização midiática que aprimorem e sensibilizem os participantes das redes sociais também podem ser úteis.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

Por fim, Whyte (2020a) acrescenta que, para que a democracia funcione de maneira eficaz, a informação deve ser disponibilizada ao público de forma que seja possível julgar sua credibilidade, origem e qualidade. No nível mais básico, para que o discurso seja democrático, devem existir métodos que tornem razoavelmente fácil saber de onde a informação provém. Isso significa que interlocutores sociais e políticos não devem ser capazes de ocultar totalmente sua identidade em relação ao discurso público.

Além disso, as fontes factuais da informação devem ser observáveis por meio de uma desconstrução razoável da retórica, opinião e cobertura jornalística analisadas. Mesmo quando há informações limitadas sobre determinado assunto, a cobertura repetitiva por fontes independentes e a contextualização tanto em análises midiáticas quanto em ambientes sociais ajudam a identificar e definir elementos significativos do foco do debate. A inibição de um ecossistema razoavelmente complexo que possibilite a investigação e a interpretação leva à dominação de poucas perspectivas, sem que haja capacidade social para explorar as nuances da questão.

A exploração de fatores humanos e tecnológicos em campanhas de desinformação

A utilização de desinformação nos conflitos internacionais não é uma novidade. Contudo, a franca transição das comunicações para a rede mundial de computadores e o surgimento de tecnologias disruptivas têm direcionado esse tipo de ação para novos domínios, aumentando eficiência e furtividade ao mesmo tempo que reduz custos, trazendo, assim, possibilidades de interferência externa em níveis antes inatingíveis sem o emprego de forças cinéticas.

Os resultados encontrados mostram que Estados-nações estão explorando vieses cognitivos e emoções para aumentar a eficácia das ações de desinformação digital. Isso ocorre particularmente durante períodos de crise e tensões globais, quando as populações ficam vulneráveis e consequentemente mais suscetíveis à desinformação. Os efeitos acabam por transcender a individualidade, produzindo consequências em escala populacional.

Flagra-se particularmente preocupante a capacidade destas campanhas em desgastar a confiança dos cidadãos em informações oficiais oriundas de instituições acadêmicas e estatais, aumentando a proliferação de ciência de baixa qualidade e de narrativas falaciosas, semeando desconfiança e gerando polarização. A possibilidade de atores maliciosos ofuscarem a própria forma como a realidade se apresenta aos indivíduos demonstra a sofisticação das

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

estratégias empregadas para interferir em processos decisórios adversários.

Como introduzido, verifica-se que tecnologias como mídias sociais e Inteligência Artificial têm sido protagonistas nas operações contemporâneas de desinformação voltadas à interferência externa, tornando-se vetores preferenciais para a manipulação da opinião pública. A difusão de conteúdos falsos ou distorcidos ocorre em escala e velocidade inéditas, sustentada por algoritmos de recomendação e engajamento e práticas de compartilhamento entre pares que conferem aparência de legitimidade e autenticidade à informação manipulada.

Saturar as redes com narrativas alternativas, teorias conspiratórias e discursos polarizadores visa não apenas confundir, mas moldar percepções e criar divisões internas. Soma-se a isso o advento dos *deep fakes* e outras formas de geração de conteúdo sintético que permitem criar publicações visuais e sonoras de alta credibilidade; além dos *bots* que ampliam a capacidade de disseminação e interação, impulsionando mensagens, silenciando opositores e forjando consensos.

Destaca-se também que parece haver uma propensão à orquestração na execução destas operações: de um lado, agentes estatais que planejam e supervisionam a campanha; de outro, "milícias digitais" (voluntárias, amadoras ou profissionais) e cidadãos comuns que, vitimados pela desinformação ou movidos por afinidade ideológica, atuam como amplificadores espontâneos. A combinação entre automação, terceirização e mobilização social descentralizada confere às operações cibernéticas de interferência externa um alto grau de resiliência e dificuldade de atribuição, tornando mais complexa a atuação da nação-alvo em ações de contrainteligência.

No que diz respeito ao enfrentamento dessa ameaça, tendo em vista o avanço rápido e constante das tecnologias supracitadas, uma modelagem de táticas centradas no ser humano para a detecção de campanhas de desinformação parece ser o caminho mais promissor a longo prazo. Conscientizar e capacitar a população para essa tarefa demanda a integração de medidas jurídicas, tecnológicas e sociais. Isso implica, por parte do Estado, fortalecer marcos legais contra a desinformação e instituir parcerias entre governo e sociedade civil, incluindo o incentivo ao desenvolvimento de agências independentes de checagem de fatos. Requer, ainda, políticas públicas que abordem alfabetização digital e midiática e mecanismos de denúncia comunitária. A população mais vulnerável deve ser o público-alvo dessas ações, especialmente jovens, idosos e cidadãos com baixa escolaridade que acabam se informando sobre

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

temas relevantes apenas por vídeos, imagens e áudios veiculados por aplicativos de mensageria e mídias sociais.

Entretanto, o Estado não pode aguardar até que a população esteja consciente e capacitada. Tampouco pode transferir aos cidadãos a responsabilidade total da neutralização dessas ameaças. É necessário proteger-se em camadas. Nesse sentido, parece salutar a delegação desta incumbência aos serviços de inteligência, uma vez que possuem o mandato legal e a expertise de contrainteligência necessários para lidar com ameaças externas em ambiente físico e virtual.

Oferecer ao público um serviço oficial de checagem de fatos por parte de agências de inteligência - considerando-se um regime democrático, evidentemente - poderia conferir mais agilidade, profissionalismo e precisão no combate à desinformação digital para fins de interferência externa. Esses órgãos - que já acompanham temas e narrativas promovidos por adversários estrangeiros a fim de identificar padrões, objetivos e indicadores de ameaça - poderiam produzir e difundir alertas públicos através de um portal online, identificando e refutando informações falaciosas que representassem risco à soberania nacional e ao estado democrático de direito. Além disso, poderiam desenvolver e disponibilizar soluções para a identificação de *deep fakes* de vídeo, áudio e de imagens sintéticas ou adulteradas, auxiliando a população na detecção de conteúdo forjado.

Em conclusão, acrescenta-se que fortalecer a governança da informação representa o fortalecimento dos próprios alicerces do Estado diante das crescentes tentativas de interferência externa. A proteção da integridade informacional se mostra, assim, não apenas uma necessidade técnica, mas uma questão estratégica de soberania nacional e preservação democrática.

Conclusão

Ao conduzir uma revisão sistemática da literatura para compreender como Estados-nações empregam a desinformação como instrumento de interferência externa, este trabalho demonstra que este tipo de ação constitui uma das mais preocupantes ameaças contemporâneas à soberania e à estabilidade democrática. Campanhas maliciosas exploram vulnerabilidades cognitivas e emocionais, utilizando *bots*, mídias sociais e Inteligência Artificial para ampliar o alcance e a credibilidade de narrativas enganosas. Como resultado, tem-se na nação-alvo um ambiente informacional em que discernir entre o que é ou não verdadeiro se torna uma tarefa complexa.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

Frente a esse cenário, a pesquisa reafirma que o enfrentamento à desinformação exige uma resposta que combine instrumentos jurídicos, tecnológicos e educacionais. Não se trata apenas de combater a desinformação após sua difusão, mas de fortalecer a resiliência da sociedade de maneira preventiva. Isso inclui desde a formulação de marcos regulatórios que responsabilizem perpetradores e patrocinadores até políticas públicas de alfabetização digital voltadas à população mais vulnerável.

Ao mesmo tempo, destaca-se a necessidade de envolver a inteligência de Estado nesse esforço. As agências de inteligência, pela natureza de sua missão e por sua capacidade técnica, podem colaborar na detecção antecipada, obstrução e neutralização de campanhas adversas. A criação de canais oficiais de checagem de fatos por estes órgãos, aliada à disponibilização de soluções de identificação de *deep fakes* e outros conteúdos forjados, representa uma forma de auxiliar diretamente a população nacional. Sugestões de pesquisas futuras caminham no sentido de desenvolver metodologias que viabilizem esse tipo de atendimento à sociedade.

Conclui-se, portanto, que o fortalecimento da governança da informação deve ser compreendido como um imperativo de soberania e de segurança nacional. Preservar a integridade do ecossistema informacional é, assim, preservar a própria democracia, não apenas contra a desinformação em si, mas contra a corrosão silenciosa da confiança que sustenta o pacto social e a legitimidade das instituições.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

Referências

ABIN (Agência Brasileira de Inteligência). 2023. Doutrina da Atividade de Inteligência. Brasília: ABIN. Governo do Brasil. https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/doutrina/Doutrina-da-Atividade-de-Inteligencia-2023.

Ambros, Christiano Cruz. 2024. "Guerra cognitiva e operações cibernéticas de influência: vieses cognitivos como tática de combate." Revista Brasileira de Inteligência, no. 19: e2024.19.252. https://doi.org/10.58960/rbi.2024.19.252.

Brasil. 2017. Estratégia Nacional de Inteligência. Decreto de 15 de dezembro de 2017. Presidência da República. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/legislacao/politica-nacional-de-inteligencia-1/ENINT.pdf

Brasil. 2016. Política Nacional de Inteligência. Decreto nº 8.793, de 29 de junho de 2016. Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm (acesso em 10 de julho de 2025).

Cartwright, Barry, Richard Frank, George Weir, e Karmvir Padda. 2022. "Detecting and Responding to Hostile Disinformation Activities on Social Media Using Machine Learning and Deep Neural Networks." Neural Computing and Applications 34: 15141–15163. https://doi.org/10.1007/s00521-022-07296-0.

la Cour, Christina. 2020. "Theorising Digital Disinformation in International Relations." International Politics 57: 704–723. https://doi.org/10.1057/s41311-020-00215-x.

DiResta, Renée, Shelby Grossman, e Alexandra Siegel. 2021. "In-House vs. Outsourced Trolls: How Digital Mercenaries Shape State Influence Strategies." Political Communication 39, no. 2: 222–253. https://doi.org/10.1080/10584609.2021.1994065.

Duarte, Felipe Pathé. 2024. "'Information Disorder' Campaigns in Natural Hazards and Extreme Events – A Form of Foreign Influence and a Hybrid Threat?" Janus.net 15, no. 1: 322–334. https://doi.org/10.26619/1647-7251.15.1.18.

García Santamaría, Sara, Paolo Cossarini, Eva Campos-Domínguez, e Dolors Palau-Sampio. 2024. "Unraveling the Dynamics of Climate Disinformation: Understanding the Role of Vested Interests, Political Actors, and Technological Amplification." Observatorio (OBS) 18, no. 6. https://doi.org/10.15847/obsOBS18520242605.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

Ivan, Cristina, Irena Chiru, e Rubén Arcos. 2021. "A Whole of Society Intelligence Approach: Critical Reassessment of the Tools and Means Used to Counter Information Warfare in the Digital Age." Intelligence and National Security 36, no. 4: 495–511. https://doi.org/10.1080/02684527.2021.1893072.

Işık, İrem, Ömer F. Bildik, e Tayanç T. Molla. 2022. "Securing Elections through International Law: A Tool for Combatting Disinformation Operations?" Journal of Strategic Security 15, no. 4: 106–125. https://doi.org/10.5038/1944-0472.15.4.2033.

Katagiri, Nori. 2023. "Democracy, Firms, and Cyber Punishment: What Cyberspace Challenge Do Democracies Face from the Private Sector?" Australian Journal of International Affairs 77, no. 5: 528–547. https://doi.org/10.1080/10357718.2023.2274443.

Kumar, Saurabh, Valerio La Gatta, Andrea Pugliese, Andrew Pulver, V. S. Subrahmanian, Jiazhi Zhang, e Youzhi Zhang. 2025. "Reinforcement-Learning Based Covert Social Influence Operations." In Proceedings of the ACM on Web Conference 2025 (WWW '25), 2435–2449. https://doi.org/10.1145/3696410.3714729.

Lapke, Michael, e Amy Browning. 2024. "Exploring the Intersection of Cyberthreats and Democratic Backsliding." AMCIS 2024 Proceedings 15. https://aisel.aisnet.org/amcis2024/soc_inclusion/social_inclusion/15.

López-Cantos, Francisco. 2024. "The Drone Warfare: Fact-Checking, Fake-Pictures and Necropolitics." Cogent Social Sciences 10, no. 1. https://doi.org/10.1080/23311886.2024.2426706.

Megiddo, Tamar. 2020. "Online Activism, Digital Domination, and the Rule of Trolls." Columbia Journal of Transnational Law 58: 394. https://doi.org/10.2139/ssrn.3459983.

Paterson, Thomas, e Lauren Hanley. 2020. "Political Warfare in the Digital Age: Cyber Subversion, Information Operations and 'Deep Fakes.'" Australian Journal of International Affairs 74, no. 4: 439–454. https://doi.org/10.1080/10357718.2020.1734772.

Saeidnia, Hamid Reza, Elaheh Hosseini, Brady Lund, Maral Alipour Tehrani, Sanaz Zaker, e Saba Molaei. 2025. "Artificial Intelligence in the Battle against Disinformation and Misinformation: A Systematic Review of Challenges and Approaches." Knowledge and Information Systems 67: 3139–3158. https://doi.org/10.1007/s10115-024-02337-7.

Smith, Tiffany. 2021. "The Infodemic as a Threat to Cybersecurity." The International Journal of Intelligence, Security, and Public Affairs 23, no. 3: 180–196. https://doi.org/10.1080/23800992.2021.1969140.

Revista Brasileira de Inteligência
2025 • nº 20 • e2025.20.287
ISSN 2595-4717

Vasist, Pramukh Nanjundaswamy, e Satish Krishnan. 2024. "Powered by Innovation, Derailed by Disinformation: A Multi-Country Analysis of the Influence of Online Political Disinformation on Nations' Innovation Performance." Technological Forecasting and Social Change 199: Article 123029. https://doi.org/10.1016/j.techfore.2023.123029.

Wagnsson, Charlotte, Albin Östervall, e Anton Angwald. 2025. "Naming the Enemy: How to Fortify Society against Foreign Disinformation while Avoiding Excessive Vigilance to Reliable Media." Humanities and Social Sciences Communications 12: 803. https://doi.org/10.1057/s41599-025-04844-6.

Watney, Murdoch. 2023. "Legal Response to Social Media Disinformation on National Level." In Proceedings of the 22nd European Conference on Cyber Warfare and Security, 525–532. https://doi.org/10.34190/eccws.22.1.1106.

Whyte, Christopher. 2020a. "Cyber Conflict or Democracy 'Hacked'? How Cyber Operations Enhance Information Warfare." Journal of Cybersecurity 6, no. 1: Article tyaa013. https://doi.org/10.1093/cybsec/tyaa013.

Whyte, Christopher. 2020b. "Of Commissars, Cults and Conspiratorial Communities: The Role of Countercultural Spaces in 'Democracy Hacking' Campaigns." First Monday 25, no. 4. https://doi.org/10.5210/fm.v25i4.10241.

Whyte, Christopher. 2020c. "Protectors without Prerogative: The Challenge of Military Defense against Information Warfare." Journal of Advanced Military Studies 11: 166–184. https://doi.org/10.21140/mcuj.2020110108.

Wu, H. Denis. 2023. "Post-Truth Public Diplomacy: A Detrimental Trend of Cross-National Communication and How Open Societies Address It." The Journal of International Communication 29, no. 1: 20–38. https://doi.org/10.1080/13216597.2022.2162099.