Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

Christiano Cruz Ambros[1]
ORCID 0009-0008-4044-1923

GUERRA COGNITIVA E OPERAÇÕES CIBERNÉTICAS DE INFLUÊNCIA: VIESES COGNITIVOS COMO TÁTICA DE COMBATE

https://doi.org/10.58960/rbi.2024.19.252

Ambros, Christiano Cruz. 2024. "Guerra Cognitiva e operações cibernéticas de influência: vieses cognitivos como tática de combate". *Revista Brasileira De Inteligência*, n.19: e2024.19.252. https://doi.org/10.58960/rbi.2024.19.252.

Recebido em 05/09/2024
Aprovado em 29/11/2024
Publicado em 18/12/2024

1 Doutor em Ciência Política pela Universidade Federal do Rio Grande do Sul (UFRGS). Pesquisador associado do Núcleo de Pesquisa em Inteligência (NUPI) da Escola de Inteligência (ESINT).

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

GUERRA COGNITIVA E OPERAÇÕES CIBERNÉTICAS DE INFLUÊNCIA: VIESES COGNITIVOS COMO TÁTICA DE COMBATE

Resumo

O objetivo deste artigo é apresentar o conceito de guerra cognitiva e demonstrar como a exploração instrumental de vulnerabilidades cerebrais, como os vieses cognitivos, em operações cibernéticas de influência é basilar para o termo. Em dezembro de 2020, o Comando Aliado de Transformação da OTAN divulgou um relatório sobre a guerra cognitiva, sugerindo a adição de um sexto domínio operacional, o domínio cognitivo, aos já estabelecidos domínios terrestre, marítimo, aéreo, espacial e cibernético. A crescente atenção dos formuladores de estratégia e dos tomadores de decisão ao caos informacional e à degradação do ambiente social e institucional tem aumentado a demanda por compreensão sobre a guerra cognitiva. É necessário, assim, que o Brasil também discuta o conceito de forma crítica e autônoma. Por meio da análise de guerra cognitiva em referências doutrinárias e na literatura especializada, busca-se compreender os núcleos conceituais do termo. Busca-se demonstrar o papel da exploração de vieses cognitivos em operações cibernéticas de influência apresentando exemplos de campanhas de desinformação. Conclui-se que a guerra cognitiva conta com aspectos distintivos em relação a outros conceitos e que carrega potencial disruptivo nos conflitos em termos operacionais e táticos, com implicações na dimensão estratégica.

Palavras-chave: Guerra Cognitiva, viés cognitivo, guerra de informação, operações de influência, operações cibernéticas de influência

COGNITIVE WARFARE AND CYBER INFLUENCE OPERATIONS: COGNITIVE BIASES AS A COMBAT TACTIC

Abstract

The aim of this article is to introduce the concept of cognitive warfare and demonstrate how the instrumental exploitation of vulnerabilities in the brain, such as cognitive biases, in cyber influence operations is fundamental to the term. In December 2020, NATO's Allied Command Transformation released a report on cognitive warfare, suggesting the addition of a sixth operational domain, the cognitive domain, to the already established land, sea, air, space, and cyber domains. The growing attention of strategy designers and decision makers to informational chaos and the degradation of the social and institutional environment has increased the demand for the understanding of cognitive warfare. It is therefore also necessary for Brazil to discuss the concept, critically and autonomously. Through the analysis of cognitive warfare in doctrinal references and specialized literature, we seek to understand the conceptual cores of the term. The conclusion is that cognitive warfare has distinctive aspects in relation to other concepts, and that it carries disruptive potential in conflicts, in operational and tactical aspects, with implications to the strategic dimension.

Keywords: *Cognitive warfare, Cognitive bias, Information warfare, Influence operations, Cyber influence operations*

GUERRA COGNITIVA Y OPERACIONES CIBERNÉTICAS DE INFLUENCIA: SESGOS COGNITIVOS COMO TÁCTICA DE COMBATE

Resumen

El objetivo de este artículo es presentar el concepto de la guerra cognitiva y demostrar cómo la explotación instrumental de las vulnerabilidades cerebrales, como los sesgos cognitivos, en las operaciones de ciberinfluencia es fundamental para el término. En diciembre de 2020, el Mando Aliado de Transformación, de la OTAN, publicó un in-

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

forme sobre la guerra cognitiva, sugiriendo la adición de un sexto dominio operativo, el dominio cognitivo, a los dominios terrestre, marítimo, aéreo, espacial y cibernético ya establecidos. La creciente atención de los estrategas y los tomadores de decisiones al caos informativo y la degradación del entorno social e institucional ha aumentado la demanda por la comprensión de la guerra cognitiva. Por lo tanto, es necesario que Brasil también discuta el concepto de manera crítica y autónoma. A través del análisis de la guerra cognitiva en referencias doctrinales y literatura especializada, buscamos comprender los núcleos conceptuales del término. Se concluye que la guerra cognitiva tiene aspectos distintivos en relación con otros conceptos y que acarrea un potencial disruptivo en los conflitos, en términos operativos y tácticos, con implicaciones en la dimensión estratégica.

Palabras clave: *Guerra cognitiva, Sesgo cognitivo, Guerra de información, Operaciones de influencia, Operaciones de influencia cibernética.*

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

Introdução

O conceito de guerra cognitiva tem sido discutido na última década como uma mudança incremental, mas significativa, na forma de condução de conflitos, especialmente no contexto das transformações tecnológicas e da crescente importância das dimensões psicológicas e informacionais na guerra moderna (Giordano 2017a; Giordano 2017b; Giordano 2017c; Bienvenue et al. 2018; Hoffman 2018). Inicialmente discutido como uma continuidade da guerra de informação e da guerra cibernética, o termo tomou traços distintivos em 2020, com a publicação de relatório do Comando Aliado de Transformação (ACT) da Organização do Tratado do Atlântico Norte (OTAN), que propõe considerar o domínio cognitivo como um novo domínio que complementa os tradicionais – terra, mar, ar, espaço e cibernético.

Há décadas operações de influência são parte da estratégia e da prática da competição entre potências, em especial dos Estados Unidos da América (EUA), Rússia e China. A manipulação do ambiente informacional para modificar ou manter o comportamento do alvo não é algo novo. A Guerra Fria (1947-1991) nos traz inúmeros exemplos de operações desse tipo executadas não só pelos EUA e Rússia, mas diversos outros países. A mudança está na transformação do domínio cibernético e o crescente conhecimento científico sobre o funcionamento do cérebro, o que aumentam as possibilidades e incentivos para conduzir a guerra cognitiva.

Novas tecnologias, por um lado, 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. Por outro, a neurociência e a psicologia cognitiva têm avançado na compreensão dos mecanismos cognitivos e emocionais que influenciam na percepção, memória, julgamento e tomada de decisões dos indivíduos.

O objetivo da guerra cognitiva é a manipulação do comportamento por meio da alteração da cognição do alvo. Isso pode ser executado interferindo diretamente nas sinapses químicas e elétricas, por meio de agentes farmacológicos e biológicos, toxinas orgânicas e dispositivos tecnológicos (Giordano 2021). A abordagem direta trata do desenvolvimento de armas neurológicas possibilitado pelos avanços da neurociência (Ambros 2024). A outra forma de modificar o processamento de informações é por meio da exploração intencional das vulnerabilidades do cérebro, como os vieses cognitivos. A abordagem indireta, que é o foco desse artigo, trata da instrumentalização da psicologia cognitiva com intenção de manipular o alvo, utilizando princi-

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

palmente as mídias sociais como veículo.

A atenção ao domínio cognitivo é crescente em diversos países, o que é refletido em mudanças doutrinárias, investimentos em tecnologia e reorganização institucional. O Japão tratou da guerra cognitiva como ameaça crescente na Estratégia Nacional de Segurança 2022 (Japão 2022a) e na Estratégia Nacional de Defesa 2022 (Japão 2022b). A Suécia criou, em 2022, a Agência de Defesa Psicológica (MPF), uma organização civil com a missão de se contrapor a operações de influência, principalmente aquelas que utilizam campanhas de desinformação online, que manipulem a percepção, comportamento e tomada de decisão no país (Psychological Defence Agency 2024). As Forças de Defesa da Austrália (ADF), em agosto de 2024, reposicionaram seu foco na guerra cognitiva e informacional ao estabelecer o Comando Cibernético como um novo comando dentro do Grupo de Capacidades Conjuntas (JCG) (Austrália 2024). Esses países reconhecem que a guerra contemporânea não se limita às dimensões físicas ou cibernéticas de batalha, mas se estende na infraestrutura cognitiva conjunta do país por meio da influência na percepção individual e coletiva.

É importante, nesse sentido, compreender como o conceito de guerra cognitiva tem sido empregado por diferentes países para motivar modificações organizacionais e doutrinárias. Não pretendemos, assim, abordar nesse artigo a pertinência teórica da utilização de termos adjetivos da guerra, como cognitiva, de informação ou cibernética. Debate-se muito sobre a distinção entre essas novas categorias e as já consolidadas, bem como a relevância prática desses conceitos para os estudos sobre a guerra e reconhece-se a importância dessa discussão no campo dos estudos estratégicos (Duarte 2020; Diniz 2024). O que se busca aqui é analisar como o conceito vem sendo apresentado em discussões doutrinárias, especialmente no âmbito da OTAN.

Nesse cenário, é necessário que o Brasil discuta a guerra cognitiva de forma crítica e autônoma. A compreensão e o debate sobre esse conceito são fundamentais para o desenvolvimento de estratégias que protejam os interesses nacionais e assegurem a soberania cognitiva do país. Ignorar ou subestimar a importância da guerra cognitiva pode deixar o Brasil vulnerável à influência externa e comprometer sua posição no cenário internacional. Portanto, uma análise aprofundada e independente desse tema é essencial para a formulação de políticas de inteligência e defesa.

> Esse artigo tem como objetivo principal analisar o conceito de guerra cognitiva, demonstrando como as operações cibernéticas de influência e a exploração de vieses cognitivos do alvo são centrais para compreender o termo. Para atingir esse objetivo, empregamos metodologia qualitativa

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

> (Keman, Kleinnijeh e Pennings 2003) como forma de organizar logicamente a investigação, revisando a literatura especializada e manuais doutrinários para definir conceitos e relacioná-los em uma rede nomológica (Jaccard e Jacoby 2010).

Dividimos, assim, o artigo em três seções. Na primeira, tratamos dos conceitos de guerra cognitiva, de informação e cibernética, buscando apontar as similaridades e diferenças entre eles. A segunda seção apresenta os conceitos de operações de influência e operações cibernéticas de influência, demonstrando quais as principais táticas e técnicas utilizadas em campanhas de desinformação. Finalmente, a terceira seção apresenta exemplos de operações cibernéticas de influência que se utilizaram da instrumentalização de vieses cognitivos para atingir seus objetivos.

Guerra cognitiva, guerra de informação e guerra cibernética

Em 2020, o Comando Aliado de Transformação (ACT) da Organização do Tratado do Atlântico Norte (OTAN) divulgou um relatório inovador que introduz o conceito de guerra cognitiva, sugerindo a necessidade de expandir os domínios operacionais da aliança para incluir um sexto domínio: o domínio humano cognitivo. Além dos cinco domínios tradicionais – terra, mar, ar, espaço e cibernético – o relatório argumenta que as guerras modernas exigem atenção às dimensões cognitivas do conflito.

François du Cluzel (2020), autor do relatório, destaca que a guerra cognitiva envolve a manipulação do comportamento humano por meio da modificação do processamento de informações. Utilizando princípios da neurociência, psicologia e tecnologia, essa forma de guerra explora vulnerabilidades cognitivas para moldar opiniões, criar confusão, disseminar desinformação e, eventualmente, enfraquecer a coesão social e política de um adversário.

A guerra cognitiva objetiva alterar a forma como o cérebro processa informação, a transforma em conhecimento e a emprega em ação, e não necessariamente com qual informação o alvo está sendo abastecido. Não se trata de manipular o conteúdo ou controlar o fluxo informacional para formar uma narrativa que racionalmente será consumida pelo alvo, mas sim de empregar tecnologias, com ênfase nas cibernéticas, que distorçam os seus mecanismos cognitivos de percepção, julgamento e memória (Cluzel 2020).

Nesse sentido, a guerra cognitiva inova não só um novo patamar em termos da manipulação do ambiente informacional, mas, principalmente, introduz a cognição humana como uma nova dimensão de disputa por comando e controle. No seu núcleo operacional estão táticas para influenciar compor-

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

tamentos que exploram falhas cognitivas do alvo. Assim, por um lado, tem-se o domínio cibernético como infraestrutura comunicacional disponível, o advento das mídias sociais como novo veículo para a disseminação de informações em massa e o engajamento da audiência alvo como reprodutora orgânica da manipulação informacional. Por outro, observa-se o crescente conhecimento em relação ao funcionamento do cérebro sendo convertido para aplicações militares dentro de processo de militarização da neurociência (Giordano 2021).

Por vezes, aspectos da guerra cognitiva parecem se sobrepor aos termos de guerra de informação e de guerra cibernética (Yun e Kim 2022). Essa sobreposição dos termos se daria especialmente porque, na guerra cognitiva, o objetivo é modificar o processo cognitivo com a finalidade de exercer influência sobre grupos ou indivíduos por meio da manipulação de informações – objetivo da guerra de informação- disseminadas, principalmente, no espaço cibernético, que é domínio da guerra cibernética. Entretanto, a delimitação conceitual de guerra cognitiva permite constatar diferenças estratégicas e operacionais em relação aos outros dois termos que demonstram a utilidade e pertinência no emprego do conceito.

A guerra de informação é um conceito que, apesar de amplamente discutido, ainda carece de um consenso claro entre estudiosos e profissionais da área. Essa falta de concordância decorre da complexidade e da amplitude do termo, que engloba uma variedade de práticas doutrinárias e estratégias envolvendo o controle do fluxo informacional. O termo começou a ser amplamente empregado como parte de um fenômeno midiático, em tempos de paz e de conflito, o que torna sua análise mais desafiadora. Como resultado, a guerra de informação está envolta em uma "névoa de conceitos" (Walker 2024), onde diferentes interpretações e abordagens coexistem, criando confusão e dificultando a formulação de definições e doutrinas.

Ao fim dos 1980, o termo guerra de informação começou a ser amplamente discutido no ambiente acadêmico e militar dos EUA e tornou-se um guarda-chuva para abrigar diferentes termos militares, como guerra de comando e controle, operações cibernéticas, guerra eletrônica, conflitos centrados em redes, segurança operacional e informacional e operações psicológicas (Huhtinen 2007). Apesar das diversas concepções, com escopo mais ou menos amplo, o núcleo conceitual do termo traz o conflito ou disputa entre dois ou mais grupos no ambiente informacional (Wanless e Pamment 2019). Esses grupos utilizam um leque de medidas e ações que objetivam proteger, explorar, corromper, negar ou destruir informação ou recursos informacionais para atingir vantagem ou objetivo significativo sobre o adversário (Cordey 2019).

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

Em geral, essas ações seriam divididas em duas frentes principais (Huhtinen 2007). No domínio informacional, a guerra de informação incluiria operações psicológicas, dissimulação, desinformação, guerra na mídia, comunicação estratégica e gerenciamento de percepção para a manipulação dos alvos[1]. E, no domínio cinético, a guerra de informação abarcaria operações cibernéticas com impactos físicos e guerra eletrônica para a disrupção e destruição das infraestruturas de informação e comunicação. Conforme Cluzel (2021, 6), a guerra de informação tem como objetivo controlar o fluxo de informações, tendo sido concebida, em grande parte, para apoiar os objetivos estabelecidos pelas missões tradicionais das forças militares, com o propósito principal de gerar efeitos letais e cinéticos no campo de batalha.

Na doutrina militar estadunidense, o termo não foi oficialmente definido em um manual próprio. Recentemente, o manual de operações do Exército dos EUA definiu que:

> No contexto da ameaça, a guerra da informação refere-se ao uso orquestrado de atividades de informação por uma ameaça (como operações no ciberespaço, guerra eletrônica e operações psicológicas) para alcançar objetivos. Operando sob um conjunto diferente de ética e leis em relação aos Estados Unidos, e sob o manto do anonimato, ameaças equivalentes conduzem a guerra da informação de forma agressiva e contínua para influenciar populações e tomadores de decisão. Elas também podem usar a guerra da informação para criar efeitos destrutivos durante períodos de competição e crise (Estados Unidos 2022).

Para os EUA, quem realiza guerra de informação são as ameaças, sejam elas estatais ou não estatais. Essas ameaças, "por terem menos restrições legais que os EUA quanto à execução de atividades informacionais, obteriam vantagens iniciais pelo emprego agressivo e contínuo em toda a faixa de operações militares, em conjunto com outros métodos" (Diniz 2024, 83).

Os EUA, por sua vez, responderiam à guerra de informação restringidos ao âmbito militar por meio de operações de informação, que são o "emprego

1 Esses conceitos são inter-relacionados. Contam com literatura especializada para seu estudo desde meados do século XX. O debate acadêmico sobre esses termos tem evoluído à medida que o impacto da tecnologia e das redes sociais aumenta o alcance e a sofisticação dessas práticas, tornando-as elementos centrais dos conflitos entre diferentes atores. Acadêmicos destacam a importância de distinguir os conceitos, ainda que frequentemente operem em conjunto, para melhor entender seu papel no cenário contemporâneo de conflitos e na formação de narrativas. Para aprofundar nos tópicos de operações psicológicas, dissimulação, desinformação e comunicação estratégica, ver Snyder (1995); Shulsky (2002); Whaley (2007); Passage (2009) e Paul (2011).

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

integrado, durante operações militares, de capacidades relacionadas à informação, concertadamente com outras linhas de operação, para influenciar, perturbar de modo a interromper, corromper ou usurpar a tomada de decisão de adversários ou de adversários potenciais, ao mesmo tempo protegendo a própria capacidade" (Estados Unidos 2016). Assim, o país desenvolveu doutrinariamente mais o conceito de operações de informação do que de guerra de informação.

O Brasil, assim como os EUA, focou mais na discussão doutrinária sobre o termo operações de informação do que o conceito de guerra de informação. De acordo com Walker (2024, 111), a guerra de informação possui um escopo mais amplo do que o das operações de informação. O conceito de guerra de informação abrange ações relacionadas a todas as formas de poder nacional, enquanto as operações de informação se referem principalmente a um esforço militar focado na manobra informacional durante uma operação. Mesmo de maneira imprecisa, doutrinariamente, nos Estados Unidos, e em menor grau no Brasil, as capacidades relacionadas à informação abarcadas pelo conceito de guerra de informação têm sido percebidas como uma função de apoio militar que facilita e possibilita as operações de combate (Derleth 2021).

Em 2014, o conceito de operações de informação foi incorporado na doutrina militar terrestre brasileira (Barboza e Teixeira 2020), no Manual de Campanha EB20-MC-10.213 (Brasil 2014) e, em 2015, passou a constar também do MD-35-G-01, *Glossário das Forças Armadas* (Brasil 2015). O exército brasileiro descreve o termo como o emprego integrado, durante operações militares, de Capacidades Relacionadas a Informações (CRI) com outras capacidades militares para influenciar, perturbar ou corromper a tomada de decisão de adversários ou potenciais adversários enquanto protege sua própria cadeia de comando e controle. Conforme consta no Manual do Exército Brasileiro para Operações de Informação de 2014:

> As Operações de Informação reúnem as CRI e outros recursos de forma permanente e de maneira coerente para criar efeitos da dimensão informacional e, por meio deles, aumentam a capacidade de oferecer vantagem operativa ao comandante. Enquanto as CRI criam efeitos individuais, as Operações de Informação enfatizam os efeitos integrados e sincronizados como essenciais para alcançar os objetivos na dimensão informacional. Uma CRI é uma ferramenta técnica ou atividade empregada em uma perspectiva da dimensão informacional, que pode ser usada para criar efeitos e condições desejáveis. Entre elas são incluídas a Inteligência, a Comunicação social, as Operações Psicológicas, a Guerra Eletrônica, a Guerra Cibernética e os Assuntos civis.

Diferentemente das operações de informação, a guerra cognitiva não é apoio e não está restrita a dimensão militar. Nesse sentido, se aproxima mais do

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

termo de guerra de informação. A guerra cognitiva, entretanto, diminui a centralidade doutrinária que as forças armadas possuem na guerra de informação, aumentando a importância de uma abordagem integrada de governo. Além disso, a guerra cognitiva não tem a dominância sobre o fluxo informacional do inimigo como principal objetivo, e sim como meio para atingir seu fim, que é a interferência no processo cognitivo do alvo.

Em contraste com a visão estadunidense, os russos entendem que o confronto informacional (*informatsionoye protivoborstvo*) não se distingue entre atividades de paz e guerra. De acordo com Cordey (2019), fronteiras entre ambientes interno e externo, níveis estratégicos, táticos e operacionais, e as formas de guerra e de coerção são difíceis de identificar. Esta abordagem é refletida na política de segurança nacional russa, que é fortemente construída na percepção de que o país está em constante cerco por potências estrangeiras e que precisa estar em conflito permanente para garantir sua sobrevivência.

Dessa forma, a abordagem russa de guerra de informação seria mais ampla e holística, envolvendo todo o aparato estatal e paraestatal, e não somente as forças militares, como é o caso da perspectiva dos EUA. O conceito de guerra cognitiva na perspectiva estadunidense vem a aproximar-se do termo russo de confronto informacional, na medida em que reconhece um estado permanente de disputa em que instrumentos de manipulação dos alvos são amplamente utilizados dentro de uma abordagem total, e não somente militar.

Por sua vez, o que se convencionou a chamar de guerra cibernética tem sua devida atenção recebida a partir de 2007 com a série de ataques cibernéticos coordenados de negação de serviço (Denial of Service –DDoS) sofrida por instituições críticas da Estônia. Esse evento coordenado "alertou a todas as autoridades de defesa do mundo sobre a existência de um fato que estava na agenda política de defesa da maioria dos países, pelo menos desde a última década do século passado, a utilização da internet como arma de guerra e espionagem" (Neto 2017). Apesar desse e de outros ataques significativos que ocorreram posteriormente, como o malware Stuxnet, utilizado para atacar o sistema operacional das centrífugas de enriquecimento de urânio do Irã em 2010, terem alimentado o termo guerra cibernética na mídia e provocado a formação de estratégias de defesa cibernética pelo mundo, não há consenso conceitual na literatura especializada (Kuehl 2009).

Ponto de convergência no termo guerra cibernética é que esse trata de uma extensão da política por meio de ações tomadas por atores estatais (ou atores não estatais com significativo suporte e direcionamento de um Estado) no

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

ciberespaço[2] (Stiennon 2015). Se refere ao uso de força tecnológica em uma disputa interestatal no espaço cibernético (Green, 2015), causando danos que incluem desde a disrupção de sistemas computacionais e infraestruturas críticas até baixas na população civil e militar.

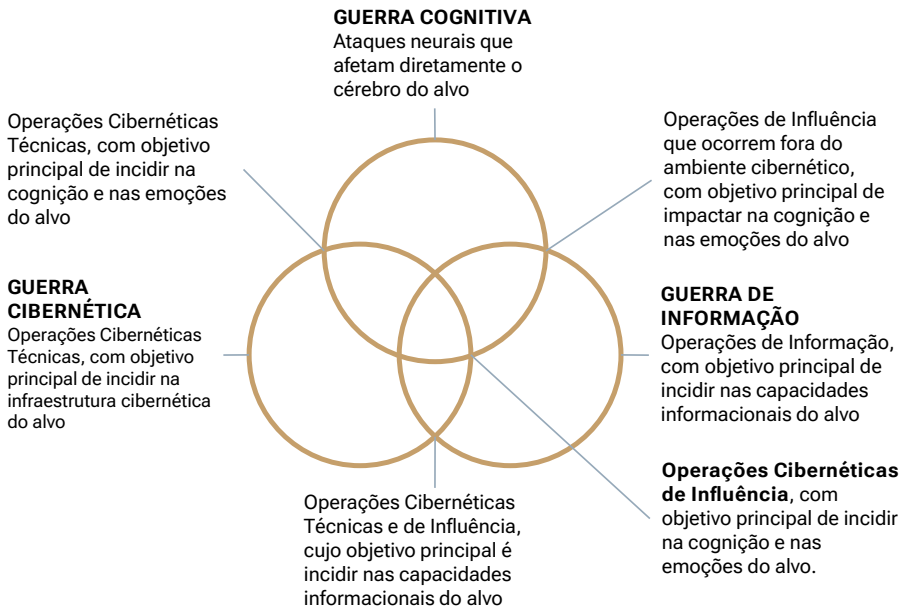
A arena em que a guerra cognitiva ocorre, apesar de ser preponderante, não é restrita ao espaço cibernético, como a guerra cibernética. Os ataques empreendidos na guerra cognitiva têm como alvo o cérebro humano, utilizando prioritariamente, mas não exclusivamente, a infraestrutura cibernética como vetor de entrega do artefato destrutivo. Ataques neurais também podem ocorrer por meio de armas de energia direta, psicotrópicos, agentes biológicos e dispositivos neurais. Essa característica difere da agressão na guerra cibernética, que tem como alvo prioritário a própria infraestrutura cibernética do adversário.

A guerra cognitiva, portanto, é constituída de atributos que a diferem da guerra de informação e da guerra cibernética. Diferentemente do que ocorre na guerra de informação, a manipulação da arena informacional não é em si mesma o objetivo da guerra cognitiva. O fluxo e o conteúdo informacional são um dos instrumentos para se manipular o processo cognitivo humano, que é o real objeto de interesse. A militarização da neurociência demonstra que a guerra cognitiva vai além da informação, buscando desenvolver tecnologias capazes de interferir no processo cognitivo a partir de dispositivos que influam diretamente na configuração neuronal do cérebro (McCreight 2022; Ambros, 2024). Além disso, em comparação com a guerra cibernética, a infraestrutura cibernética é somente um dos canais por onde a disputa pelo controle cognitivo ocorre. Diferentemente da guerra cibernética, a guerra cognitiva não objetiva impactar, manipular, obstruir ou destruir o elemento cibernético. Considerando essas observações, o Diagrama de Venn abaixo é útil para ilustrar o argumento:

2 Conforme Neto (2017) sintetiza: "O ciberespaço é um ambiente artificial caracterizado por uma complexa e não centralizada rede de emissões e transmissores de informações, composta não apenas pela Internet (rede mundial de computadores), mas também por redes privadas (intranets) e telecomunicações em geral. Utiliza meios físicos (ex: cabos de fibra ótica), wireless e espaciais (satélites)".

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

Figura 1
Diagrama de Venn entre Guerra Cognitiva, Guerra Cibernética e Guerra de Informação.



Fonte: Elaboração própria.

O ponto de convergência entre a guerra cognitiva, a guerra cibernética e a guerra de informação são as operações cibernéticas de influência. Na guerra cognitiva, o foco é alterar a forma como o cérebro do alvo percebe, processa e armazena informação, impactando em sua interpretação da realidade e no seu comportamento. Essa alteração das sinapses cerebrais pode ser feita de forma direta ou indireta. A abordagem direta é executada por meio da utilização de armas neurológicas, que modificam física ou quimicamente o cérebro para alterar seus processos biológicos (Ambros 2024). A abordagem indireta, objeto desse artigo, relaciona-se com a instrumentalização da psicologia cognitiva e é feita, prioritariamente, por meio da exploração de vieses cognitivos. Na próxima seção, expomos as características de operações de influência e de operações cibernéticas de influência, que por meio de táticas de desinformação; induzem a ocorrência de vieses cognitivos em seus alvos para atingir seus objetivos.

Operações de Influência e Operações Cibernéticas de Influência

A cognição é o processo mental pelo qual se adquire, se processa e se aplica informações e conhecimento. Cognição é como nós respondemos mentalmente a alguma forma de estímulo. Se um adversário é capaz de controlar a cognição, ele pode perturbar, manipular ou obstruir o processo de tomada de decisão, impactando na estratégia como um todo, o que é o objetivo principal

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

das operações no domínio cognitivo. Essas operações:

> [...] consideram o cérebro humano como o principal espaço de combate e focam em golpear, enfraquecer e desmantelar a vontade de lutar do inimigo, usando fraquezas psicológicas humanas como o medo, ansiedade e confusão como ponto de ruptura, explorando técnicas para criar uma atmosfera de insegurança, incerteza e desconfiança entre o inimigo, aumentando sua fricção interna e dúvida na tomada de decisão. (Baughman 2023).

Entre as principais operações no domínio cognitivo estão as operações de influência, inclusive e principalmente aquelas que ocorrem no espaço cibernético, que são as operações cibernéticas de influência. O ambiente cibernético, assim, tem agido como um facilitador e equalizador de operações de influência. O aumento da velocidade, alcance, escala, penetração e personalização da disseminação de informações em redes sociais facilitou ainda mais o uso de operações cibernéticas de influências. Elas se tornaram uma opção assimétrica e uma ferramenta para contrabalançar o poder convencional com relativo baixo custo, alta flexibilidade, baixo risco de detecção e, ainda assim, alto potencial de resultados. Essa combinação tornou as ações no espaço cibernético particularmente atrativas para vários atores.

Embora as operações cibernéticas de influência tenham se tornado táticas mais acessíveis e atrativas, isso não significa que as capacidades materiais e institucionais para executá-las sejam equivalentes entre grandes potências e outros atores. Pelo contrário, as grandes potências, devido a seus vastos recursos, infraestrutura tecnológica avançada e organizações robustas, têm a capacidade de conduzir operações cibernéticas complexas de forma mais eficaz e sustentada ao longo do tempo. Elas podem manter campanhas prolongadas e sofisticadas no ambiente cibernético, explorando a superioridade tecnológica e operando com um nível de coordenação e alcance que é dificilmente igualado por atores menores. Dessa forma, embora as operações no domínio cognitivo sejam atrativas para todos, as grandes potências ainda mantêm uma vantagem significativa em termos de escala, sofisticação e durabilidade de suas campanhas.

Operações de Influência[3] tratam da aplicação coordenada, integrada e sincronizada das capacidades nacionais diplomáticas, econômicas, militares e informacionais, com foco em influenciar decisões, percepções e compor-

3 Na literatura internacional especializada, principalmente estadunidense e europeia, é comum ver termos como *influence operations, covert influence operations, information operations e informational influence operations* quase como sinônimos. Essa confusão conceitual tem impacto na elaboração de doutrinas e na prática dos profissionais que lidam com esses fenômenos.

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

tamentos da população, de grupos particulares (como especialistas, militares ou mídia) ou de indivíduos (tomadores de decisão) (Schmidt-Felzmann 2017). De acordo com Pamment et al. (2018), elas são tentativas ilegítimas de influenciar a formação de opinião pública e o comportamento dos alvos (domesticamente ou no exterior), pois são inerentemente deceptivas e tem intenção de causar dano ou disruptura na audiência a que se dirige.

É um termo amplo que cobre vários tipos de operações no domínio informacional, incluindo tanto atividades ostensivas (como diplomacia pública e gerenciamento de mídia) quanto ações encobertas (p.e., recrutamento de formadores de opinião), que são articuladas com a intenção de impactar o público alvo para modificar ou manter percepções, aceitar visões e adotar decisões que coadunem com os interesses dos patrocinadores da operação.

Exploram diferentes aspectos das vulnerabilidades existentes na sociedade e nos indivíduos, no âmbito da formação de opinião pública, da cadeia epistêmica ligada ao sistema de mídia, educacional e empresarial e do processo político/estratégico de tomada de decisão. Como tal, se constituem não só em uma interferência no comportamento normal e na formação de opinião, mas também no processo decisório doméstico e na própria soberania dos estados.

A contraposição a operações de influência é ação típica dos órgãos estatais responsáveis pela Atividade de Inteligência, mais especificamente pela contrainteligência. A operação de influência é um tipo de ação de interferência externa, que conforme a Doutrina da Atividade de Inteligência (Brasil 2023, 72) da Agência Brasileira de Inteligência (ABIN), " 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".

As operações de influência têm se intensificado no domínio cibernético. O ciberespaço fornece a infraestrutura e as ferramentas – tanto legítimas quanto ilegítimas – para executar essas operações de maneira mais abrangente e rápida, por menor custo relativo. Da perspectiva do agressor, conduzir operações cibernéticas de influência é atrativo porque ganhos políticos e estratégicos podem ser efetivamente obtidos a menor custo do que se utilizando de meios tradicionais.

Operações cibernéticas são divididas em técnicas e de influência (Bonfanti 2019). As operações cibernéticas técnicas são geralmente referidas como

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

ataques cibernéticos e afetam as camadas lógica (programação de softwares e sistema operacional) e físicas (hardware e infraestrutura física, como cabos e servidores) do ciberespaço. As operações cibernéticas de influência agem na camada semântica do ciberespaço, ou seja, no conteúdo informacional, por meio de uma grande variedade de ferramentas e técnicas objetivando influenciar percepções e emoções da audiência, amplificando tensões políticas, diplomáticas, econômicas e militares.

A guerra cognitiva inclui operações cibernéticas de influência, mas não as operações cibernéticas técnicas, que são eminentemente parte da guerra cibernética. Essa distinção ficou confusa com os consideráveis avanços técnicos nas operações cibernéticas de influência, como o uso de redes de bots para disseminação de desinformação, ataques de DDoS ou ransomware para manipular estrategicamente narrativas que afetem a opinião pública ou a utilização de deepfakes para destruição de reputações. Ainda que nesses exemplos ocorra uso intensivo de tecnologias cibernéticas, o alvo da ação é a mente humana, diferentemente do que ocorre nas operações cibernéticas técnicas, cujo objetivo são entidades não humanas, como sistemas em rede, infraestrutura de informação ou os dados em si (Yun e Kim 2022).

Dessa forma, um ataque cibernético que causa danos físicos com a intenção de paralisar uma infraestrutura crítica, como eletricidade ou água, não tem como foco obter alguma influência cognitiva, ainda que seja possível que ocorra como efeito colateral. Se o ataque cibernético, entretanto, foi perpetrado com o objetivo de causar pânico ou minar a confiança pública no sistema, considera-se que ele tem efeito cognitivo direto. De forma similar, ataques cibernéticos cujo objetivo é mudar o resultado de eleições alterando dados de votação de forma clandestina (ou seja, sem que a ação seja percebida pelo alvo), não são ataques com efeitos cognitivos (Paikowsky e Matania 2019, 100).

A desinformação é uma das principais ferramentas utilizadas em operações cibernéticas de influência na guerra cognitiva. A desinformação não são mentiras pontuais, mas a disseminação metódica de mensagens para construção de narrativa. Em geral, busca explorar fraturas e tensões pré-existentes dentro da audiência específica que quer atingir.

Na Doutrina da Atividade de Inteligência da ABIN (Brasil 2023, 73), consta que "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. Nas redes sociais, a disseminação

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

da desinformação é feita, em geral, de modo inautêntico e coordenado".

Aprofundando mais o conceito, a desinformação pode ser vista como a combinação de uma intenção de causar dano/prejuízo com princípios de comunicação não éticos[4] explorados por técnicas específicas. No domínio cibernético, ela é composta por dois elementos: a) conteúdo informacional, que é falso, manipulado ou contextualmente distorcido; e b) comportamento inautêntico, que é o uso de bots, trolls e amplificação artificial. Uma campanha de desinformação é composta por diversas ações articuladas ao longo do tempo que buscam atingir o objetivo de forma incremental.

Os objetivos das operações cibernéticas de influência, especialmente aquelas que se utilizam de desinformação, geralmente são: i) polarizar, desestabilizar e romper a coesão social por meio da exacerbação de temas polêmicos; ii) minar a confiança nas instituições públicas e processos estabelecidos; iii) disseminar confusão, gerar exaustão e criar apatia; e iv) ganhar influência estratégica sobre o processo de tomada de decisão e a opinião pública. Para alcançar esses objetivos, busca-se criar, fomentar, destruir ou diluir uma narrativa, que é a ferramenta essencial na guerra cognitiva.

Em geral, atores adotam três estratégias principais na construção de narrativas (Pamment et al. 2018): i) a narrativa defensiva ou construtiva, que estabelece uma narrativa coerente com elementos pré-existentes e toma ações para mantê-la sólida e intocada; ii) a narrativa ofensiva ou disruptiva, que é desenhada para interromper uma ação não desejada, reduzir adesão à narrativa oponente, e perturbar ou destruir uma narrativa existente ou emergente; e a iii) narrativa diversionista, que busca reduzir a qualidade do ambiente comunicacional e informacional, com objetivo de distrair ou desengajar a audiência de um assunto central e diminuir a confiança no canal comunicacional. Para condução persuasiva das narrativas nas operações cibernética de influência, são orquestrados ataques cognitivos, que exploram ativamente as vulnerabilidades cerebrais humanas (Pocheptosov 2018). Na próxima seção, apresenta-se como vieses cognitivos são explorados em operações ciberné-

4 Os princípios comunicacionais não éticos da desinformação são os seguintes: **1. Fabricação de conteúdo:** criação ou manipulação de conteúdo, tornando-o falso. Exemplo: documento forjado, imagem manipulada, texto tirado de contexto; **2. Falsidade de identidade:** disfarçar-se de uma identidade ou falsamente atribuir conteúdo a determinada fonte. Exemplo: conta falsa em redes sociais ou um impostor; **3. Retórica desonesta:** abordagem maliciosa e com argumentos distorcidos. Exemplo: *trolls* em comentários de fóruns de debate; **4. Simbolismo:** executam ações pelo seu impacto comunicativo no ambiente informacional. **5. Apoio Tecnológico:** implementam recursos tecnológicos para distorcer o ambiente informacional. Exemplo: bots que automaticamente disseminam mensagens, dando a percepção de amplificação da narrativa.

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

ticas de influência para fortalecer estratégias de construção de narrativas e atingir os objetivos de manipulação do alvo.

Vieses Cognitivos em Operações Cibernéticas de Influência

O objetivo da guerra cognitiva é mudar ou influenciar a percepção, o julgamento e a memória do alvo, o que pode ser alcançado por meio da manipulação dos vieses cognitivos no processamento de informações. Vieses cognitivos são erros sistemáticos e repetitivos causados pelo processamento informacional heurístico, que utiliza atalhos mentais e estratégias de simplificação da informação. Os vieses ocorrem inconscientemente, de forma automática e involuntária (Kahneman, Slovic e Tversky 1982; Kahneman 2011). A maior parte deles é universal, pois são decorrentes do processo de evolução do cérebro humano (Heuer 1999).

Para serem mais convincentes e persuasivas, as narrativas criadas em operações cibernéticas de influência empregam táticas que exploram ativamente determinados vieses cognitivos. O estabelecimento da narrativa frequentemente é composto por seis táticas: i) enquadramento de um problema ou ator em perspectiva antagônica; ii) iniciativa e controle do ambiente informacional; iii) sobrecarga e distorção informacional; iv) amplificação de ameaças e manutenção constante de pressão negativa; v) oferecimento de conforto cognitivo por meio de respostas e soluções simples ao problema ou ameaça percebida; e vi) controle cognitivo em relação ao alvo.

Em relação à i) tática do enquadramento, geralmente a narrativa busca um problema ou ameaça que possa ser personificado em inimigo difuso ou específico. Esse enquadramento não necessariamente precisa ser baseado em elementos racionais. Pode conter evidências empíricas, mas apoia-se especialmente nas emoções, metáforas distorcidas e raciocínio histórico dúbio. Essa etapa passa pela avaliação profunda das vulnerabilidades dos alvos, levando em conta a cultura, experiências históricas, preconceitos, valores e interesses da audiência.

Em novembro de 2023, logo após o início da Guerra de Gaza, Israel organizou e patrocinou uma operação cibernética de influência cujos alvos eram congressistas dos EUA e a população do país (Sheera 2024). As centenas de perfis falsos ativos na plataforma X, antigo Twitter, buscavam promover narrativa pró-Israel. Enquadrando as ações de Israel como justas e legitimadas por Deus e disseminando a ideia de que os judeus estavam sendo perseguidos novamente, criando paralelismos com o holocausto durante a Segunda Guerra Mundial. Os perfis também atacavam palestinos e enquadravam o Hamas

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

como sanguinários e irracionais, não sendo possível qualquer negociação.

Entre os vieses explorados no enquadramento da narrativa estão:

- Viés de enquadramento: é a tendência de se responder ou processar informação de maneira diferente dependendo da forma como o mesmo evento é apresentado. Ou seja, informações podem ser apresentadas de diferentes formas para enquadrar aquilo que não era percebido como ameaça ou problema como tal, levando a audiência alvo a diferentes conclusões apesar de estar exposta ao mesmo conjunto de informações.

- Viés em favor de explicações causais: a mente humana busca encontrar coerência e explicações causais nos acontecimentos que nos cercam. Existe uma grande necessidade em encontrar padrões regulares e relações e ordem estabelecidas nos eventos e objetos, não se aceitando facilmente a noção de acaso ou aleatoriedade (Heuer 1999). Essa necessidade psicológica ocasiona o viés da aceitação de evidência, em que se tende acreditar mais em uma narrativa concisa, compreensível e coerente em si mesma do que nas evidências que a compõe. Ou seja, tendemos a atribuir maior ou menor confiabilidade às informações que compõe uma narrativa a depender de sua coerência interna.

- Viés de grupo: é a tendência em reconhecer-se como pertencente a um grupo e favorecer seus pares, enquanto negligencia e prejudica membros de outros grupos. Geralmente, as narrativas criadas buscam atribuir valores e crenças comuns na definição dos limites de determinado grupo, projetando naqueles que não pertencem a ele valores e crenças opostas. Ao explorar esse viés, aumenta-se a coesão interna e dissuade-se a dissidência, ao mesmo tempo que se demoniza e desumaniza o grupo colocado como antagônico.

Nas operações cibernéticas de influência, é fundamental ii) tomar a iniciativa e adiantar-se em relação ao adversário na construção da narrativa, mantendo sob controle o ambiente informacional. Isso decorre porque o cérebro tem a tendência de priorizar informações a que foi exposto primeiro. Táticas de manipulação da sequência da exposição de informações são amplificadas explorando-se diversos vieses cognitivos associados a essa tendência, principalmente o viés da ancoragem e o efeito de posição serial.

- Viés da ancoragem: envolve a seleção de um ponto inicial (a âncora)

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

no processo mental, que geralmente é a primeira informação que se recebe, e vai gradualmente ajustando as novas informações de forma a serem compatíveis com a âncora. Ainda que mais tarde se descubra que as evidências que constituem a âncora estavam incorretas, a tendência é que haja uma grande dificuldade de mudar o marco cognitivo inicial, fazendo com que, inercial e involuntariamente, o enfoque inicial seja mantido. Demonstra como somos suscetíveis às primeiras impressões e às primeiras informações a que somos expostos.

- Efeito da posição serial: a ordem em que uma informação é apresentada afeta a importância relativa atribuída a ela. Informações apresentadas primeiro e por último recebem maior atenção e são particularmente enviesadas, com tendência a subestimar informações apresentadas intermediariamente.

Em junho de 2020, três meses após a Organização Mundial de Saúde declarar a COVID-19 como uma pandemia, o Departamento de Defesa dos EUA lançou uma campanha de desinformação para diminuir a influência chinesa sobre as Filipinas (Bing e Schectman). Preocupados em adiantar-se na construção da narrativa, ao menos 300 contas falsas no antigo Twitter, atual X, foram criadas para disseminar a ideia de que o vírus era uma arma chinesa. Posteriormente, os militares estadunidenses atacaram as doações de vacinas e máscaras chinesas às Filipinas, veiculando com os mesmos perfis que essas medidas não funcionariam, pois aquilo faria parte de uma grande conspiração e que a China exigiria território filipino em troca da ajuda. A adesão a vacinação nas Filipinas foi baixa no início das campanhas de inoculação.

A iii) exposição repetida e sistemática do mesmo padrão de informações é tática usual nas operações cibernéticas de influência. As pessoas tendem a perceber e valorizar mais informações que foram recentemente e repetidamente trazidas a sua atenção, aumentando, ao longo do tempo, a confiança na veracidade daquela informação. Assim, uma das táticas utilizadas para ampliar a persuasão da narrativa é a sobrecarga informacional. O objetivo é intensificar a exposição ao tipo de informação pretendida, ao mesmo tempo que restringe ou distorce o acesso a informações pelo alvo, bloqueando ou sobrecarregando canais de informação concorrentes. Trabalha-se na lógica da curva do esquecimento de Ebbinghaus (Jindal 2023).

A privação no acesso a informações concorrentes em relação à narrativa colocada é associada ao efeito de filtro bolha, que na dimensão cibernética ocorre ao se capturar o alvo em uma bolha informacional criada por algoritmos de inteligência artificial das redes sociais que retroalimentam o alvo sempre

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

com o mesmo padrão de informações. Para promover esse contexto, são exploradas a heurística da disponibilidade, o viés da familiaridade e o efeito da verdade ilusória.

- Heurística da disponibilidade: opera na noção de que se algo pode ser lembrado com facilidade, deve ser importante, ou pelo menos mais importante do que soluções alternativas que não são tão prontamente recuperadas da memória. Sob o efeito do viés da disponibilidade, as pessoas tendem a supervalorizar informações mais recentes em seus julgamentos e, muitas vezes, que tenham maior apelo emocional, formando opiniões tendenciosas.

- Viés da familiaridade: faz com que a informação familiar seja mais facilmente recuperada da memória, impactando positivamente no julgamento, e que novas informações similares àquela informação familiar sejam percebidas e processadas de forma mais fluida.

- Efeito da verdade ilusória: é a tendência de acreditar na veracidade de informações a que o indivíduo fica repetidamente exposto. Assim, mesmo que a pessoa tenha consciência de que determinada informação é falsa, a exposição repetida ao longo do tempo torna-a mais aceitável e plausível.

A empresa Meta, em agosto de 2023, anunciou que obstruiu a maior e mais longa operação cibernética de influência ligada à China, removendo 7.700 contas falsas no Facebook e centenas de páginas e perfis inautênticos no Instagram (Paul 2023). A rede operava desde 2018, promovendo narrativas pró-chinesas e anti-americanas. Os perfis disseminaram milhares de mensagens, expondo os alvos sistematicamente ao mesmo padrão de conteúdo, com efeitos de verdade ilusória.

A iv) pressão negativa é tática utilizada para enfatizar à audiência alvo ameaças percebidas, criando-se ansiedade agressiva e dissonância cognitiva (Yun e Kim 2022). O executor da operação explora a dimensão emocional da audiência alvo, dado que as emoções são processadas mais prontamente que outros tipos de informação. O viés da negatividade, nesse sentido, é amplamente explorado, dado que as pessoas tendem a se engajar mais com emoções negativas e a responder mais rapidamente a informações que ameassem seu conforto cognitivo (Boswinkel et al. 2022). O objetivo é conduzir a audiência a buscar informações alternativas que forneçam soluções ao desconforto emocional e desordem psicológica causada pela intensificação do grau de ameaça percebida.

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

Em janeiro de 2022, semanas antes do início da invasão da Ucrânia pela Rússia, uma operação cibernética de influência foi iniciada contra a Suécia. Dezenas de vídeos sobre um potencial ataque russo sobre o país circularam repetidamente no TikTok e Twitter de crianças e adolescentes, elevando níveis de medo e ansiedade, e mobilizando pais a acionarem autoridades (Braw 2022). Os patrocinadores da ação não foram identificados, mas a motivação foi elevar a pressão negativa sobre o país, que dois anos depois decidiu abandonar sua histórica neutralidade para se juntar à OTAN.

A tática de ampliar emoções negativas é seguida pelo v) oferecimento de conforto cognitivo, por meio da produção de informações falsas ou distorcidas que disponibilize solução simples ao problema ou à ameaça, oferecendo sensação de satisfação ou realização frente às frustrações agressivas e à dissonância cognitiva. Dada a falta de alternativas informacionais percebidas, o alvo que está sofrendo de pressão negativa tende a facilmente aceitar informações de baixa qualidade ou duvidosas que o ajude a lidar com o estresse emocional e com o desequilíbrio psicológico (Yun e Kim 2022).

A coleta de dados pessoais por meio das redes sociais e as estratégias de *microtargeting*, ou seja, o desenvolvimento de algoritmos capazes de customizar a melhor mensagem de acordo com o perfil psicológico do alvo, permitem que operações de influência cibernética sejam cada vez mais direcionadas e precisas para exercer pressão negativa e oferecer conforto cognitivo à audiência. A maior compreensão psicológica do alvo permite que o viés de confirmação seja explorado de maneira bastante profunda, com a criação de peças informacionais que reforçam e confirmam ideias e crenças previamente internalizadas pelo alvo e que se coadunem com a narrativa veiculada.

O viés de confirmação, quando explorado de maneira sistêmica em uma audiência, cria câmaras de eco que reverberam as mesmas mensagens em diferentes canais informacionais dentro de um ecossistema de comunicação definido. A veiculação em massa e repetitiva de peças informacionais similares utilizando variadas comunidades online, aplicativos de mensageria e redes sociais cria uma nova percepção de realidade onde as fontes dominantes são inquestionáveis e informações concorrentes são censuradas, desautorizadas e prontamente atacadas e descartadas. Uma vez que a audiência alvo se encontra em uma câmara de eco, o efeito adesão[5] é amplamente explorado,

5 O efeito adesão (*bandwagon effect*) se refere ao fenômeno cognitivo resultante da conformidade individual à opinião da maioria do grupo à qual se pertence. Indivíduos tendem a exibir maior afinidade com informações já validadas por outras pessoas de seu grupo social, em processo de diminuição do custo cognitivo e emocional de reavaliar e questionar ideias previamente concebidas (Schmitt-Beck 2015; Knyazev & Oosterhuis 2022). Se muitas pessoas aceitam uma informação falsa como verdadeira, outras pessoas tenderão a aceitá-la também sem nem questioná-la.

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

pois o custo social e cognitivo de se questionar uma informação falsa é alto o suficiente para dissuadir qualquer atitude dissidente.

Finalmente, uma vez que a audiência está capturada, vi) o controle cognitivo, que pode ser instrumentalizado para a manipulação de comportamento, se foca na promoção do ódio, da agressividade e da rejeição a tudo que coloque em risco o conforto cognitivo obtido com a narrativa criada. Para isso, se estabelecem claras fronteiras que dividem quem é aliado e inimigo e o que é bom e mau. Nesse processo, busca-se demonizar, caricaturizar, desumanizar e criminalizar o inimigo e suas ideias, enquadrando qualquer atitude do outro lado como inerentemente negativa, dado os problemas intrínsecos do outro (Yun e Kim 2022).

Dois vieses são explorados para se otimizar a divisão de grupos:

- Erro fundamental de atribuição: é a tendência de julgar as decisões, as atitudes e os comportamentos do outro superestimando as suas disposições internas (caráter, valores, crenças, etc.) e subestimando os seus constrangimentos externos (restrições de tempo e recursos, características ambientais, etc.).

- Viés do ponto cego: quando se considera que o outro está mais sujeito a erros na avaliação de informações e tomada de decisão do que o próprio indivíduo.

O erro fundamental de atribuição é amplamente estudado no contexto do conflito árabe-israelense (Heuer 1999; Houghton 2009), buscando compreender como os atores envolvidos percebem e interpretam erroneamente o comportamento do outro. Israel acusa os palestinos de manipularem a mídia para demonizá-los perante a comunidade internacional (Baker 2014). Considerando o atual conflito em Gaza, iniciado em outubro de 2023, o caso parece ser o reverso, com algumas das principais mídias de países ocidentais utilizando técnicas narrativas para desumanizar os palestinos (Lauterbach e Shabibi 2023; Johnson e Ali 2024), inclusive com diretrizes editoriais formais que os jornalistas deveriam seguir (Lauterbach e Shabibi 2024; McGreal 2024).

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

Conclusão

O objetivo desse artigo foi apresentar como vieses cognitivos são explorados em operações cibernéticas de influência, contextualizando a discussão no âmbito do conceito de guerra cognitiva. O avanço no conhecimento sobre vieses cognitivos, advindo do avanço das ciências do cérebro, tem servido como base para a instrumentalização das falhas cognitivas cerebrais em prol de objetivos traçados por atores adversos em campanhas de influência e desinformação nas redes sociais.

A publicação em 2020 do relatório da OTAN sobre guerra cognitiva e vieses cognitivos aponta que o debate conceitual e a aplicabilidade tática desse tipo de conflito têm atingido novo patamar em termos de atenção dos formuladores de políticas e estrategistas e maturidade doutrinária militar. A guerra cognitiva não é somente um novo nome para a guerra de informação ou para guerra cibernética. Ela representa a convergência de elementos da guerra de informação expandida por noções operacionais da neurociência para a exploração de vulnerabilidades cerebrais inerentes por meio da utilização de tecnologias específicas, especialmente, mas não exclusivamente, cibernéticas.

Não foi nossa intenção aqui esgotar o debate teórico e conceitual sobre a pertinência da utilização de termos adjetivos da guerra, como de informação, cibernética ou cognitiva. Reconhece-se que essa é uma importante discussão no campo dos estudos estratégicos (Duarte 2020; Diniz 2024). Ademais, estudos recentes sugerem que seria mais produtivo para a análise acadêmica e para formulação de estratégias e tomada de decisão enquadrar o que se convém chamar de guerra cibernética como uma situação de competição e conflito permanente entre atores de Inteligência (Chesney e Smeets 2023). A ausência de intenção de produção de impacto cinético direto e a necessidade de uma abordagem integral de governo seriam as principais razões para o reenquadramento conceitual da guerra cibernética, o que, seguindo a lógica, seria estendido aos termos de guerra de informação e guerra cognitiva.

Tampouco foi o objetivo desse artigo demonstrar preponderância estratégica das ações no domínio cognitivo em relação ao domínio cinético. A Guerra da Ucrânia tem levantado hipóteses sobre os limites da guerra cognitiva em fornecer vantagem estratégica de forma independente sem estar atrelada a resultados de confrontos no domínio cinético, colocando em dúvida a real importância do domínio cognitivo. As operações cibernéticas de influência, segundo Takagi (2022), servem mais como estratégia de apoio de operações no ambiente físico do que como um meio para alcançar objetivos estratégicos. Além disso, Maschmeyer et al. (2023) ainda apontam os limites de operações

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

de influência em redes sociais na Guerra da Ucrânia, demonstrando que a utilização de mídias tradicionais para operações de influência tem alcançado maiores resultados do que operações veiculadas pelas mídias digitais.

Ainda que essas limitações devam ser levadas em consideração, elas não invalidam a importância de compreender mais sobre guerra cognitiva. Argumentamos que esse tipo de guerra (seja apropriado caracterizá-la- como guerra ou não) engloba aspectos fundamentais que a tornam um fenômeno com características próprias relevante de ser aprofundado em futuras pesquisas. Entre essas particularidades estão a ampliação e barateamento da capacidade tecnológica de manipulação do ambiente informacional, o crescente conhecimento sobre neurociência e sua aplicação em tecnologias militares e a incorporação oficial em doutrinas e estratégias militares.

Para aprofundar o entendimento sobre a natureza e as implicações da guerra cognitiva nos conflitos contemporâneos, do ponto de vista político-institucional, futuras pesquisas devem discutir sobre a abordagem integral de governo e o papel dos órgãos de Inteligência em lidar com o fenômeno. Do ponto de vista estratégico, é preciso análise atenta ao desenvolvimento dos programas nacionais de militarização das ciências do cérebro e sua materialização em novas tecnologias. Da perspectiva tático-operacional, faz-se necessário estudos de caso de operações cibernéticas de influência em conflitos atuais e como a instrumentalização dos vieses cognitivos impacta nos resultados dessas operações. Finalmente, o estudo sobre os impactos da Inteligência Artificial na guerra cognitiva é decisivo para a compreensão da futura dimensão dos conflitos no domínio cognitivo.

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

Referências

Ambros, Christiano Cruz. 2024. "Guerra Cognitiva e militarização da neurociência: programas de pesquisa em neurotecnologias dos Estados Unidos e da China." *Revista Brasileira de Estudos de Defesa* 11, no.1: 153-180. https://doi.org/10.26792/rbed.v11i1.75409.

Austrália. 2024. "A New Era For The Cyber Domain." https://www.defence.gov.au/news-events/news/2024-08-09/new-era-cyber-domain (Acesso em 04 de setembro 2024).

Baker, Alan (Ed.) 2014, "Palestinian Manipulation of the International Community". *Jerusalem center for Public Affairs*. https://jcpa.org/wp-content/uploads/2014/04/Palestinian_Manipulation.pdf (Acesso em 28 de novembro de 2024).

Barboza, Carlos Eduardo de Matos, e Luís Henrique Vighi Teixeira. 2020. "Resgatando a Essência das Operações de Informação na Guerra Convencional." *Army University Press*. https://www.armyupress.army.mil/Journals/Edicao-Brasileira/Arquivos/Quarto-Trimestre-2020/Resgatando-a-Essencia-das-Operacoes-de-Informacao-na-Guerra-Convencional/ (Acesso em 24 de agosto de 2024).

Baughman, Joshua. 2023 "Enhancing the Battleverse: The People's Liberation Army's Digital Twin Strategy." *Military Cyber Affairs* 6, no.1: 1-11. https://doi.org/10.5038/2378-0789.6.1.1091.

Bienvenue, Emily, Don DeBats, Maryanne Kelton, Zac Rogers e Sian Troath. 2018. "Understanding the Emergent Cognitive Battlespace." Paper presented at Australian Society of Operations Research and Defence Operations Research Symposium, National Conference, Melbourne, Australia. https://www.confer.nz/asor-dors2018/book-of-abstracts/ (Acesso em 17 de junho de 2024).

Bing, Chris, e Joel Schectman. 2024. "Pentagon ran secret anti-vax campaign to undermine China during pandemic." *Reuters*, 14 de junho. Washington, DC. https://www.reuters.com/investigates/special-report/usa-covid-propaganda/ (Acesso em 17 de junho de 2024).

Bonfanti, Matteo. 2019. "An Intelligence-based approach to countering social media influence operations." In *Romanian Intelligence Studies Review*. Bucharest: National Intelligence Academy.

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

Boswinkel, Lotje, Niel Finlayson, Johs Michaelis e Michael Rademaker. 2022. "Weapons of mass influence: Shaping atitudes, perceptions and behaviours in today's information warfare." "The Hague Centre for Strategic Studies. https://hcss.nl/report/weapons-of-mass-influence-information-warfare/ (Acesso em 18 de abril de 2023).

Brasil. 2014. *Manual de Campanha EB70-MC-10.213, Operações De Informação*. https://bdex.eb.mil.br/jspui/bitstream/123456789/11915/1/EB70MC10213.pdf (Acesso em 24 de junho de 2024).

Brasil. 2015. *Glossário Das Forças Armadas*. https://bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf (Acesso em 24 de junho de 2024).

Brasil. 2023. *Doutrina da Atividade de Inteligência*. Aprovada pela Portaria GAB/DG/ABIN/CC/PR nº1.205, 27 de novembro de 2023. Brasília: Abin.

Braw, Elisabeth. 2022. " 'War Is Coming': Mysterious TikTok Videos Are Scaring Sweden's Children." Defense One, 16 de janeiro. https://www.defenseone.com/ideas/2022/01/war-coming-mysterious-tiktok-videos-are-scaring-swedens-children/360808/ (Acesso em 17 de junho de 2024).

Chesney, Robert and Max Smeets. *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest*. Washington, D.C.: Georgetown University Press.

Cluzel, François Du. 2020. *Cognitive Warfare*. www.innovationhub-act.org/sites/default/files/2021-01/20210122_CW%20Final.pdf (Acesso em 04 de agosto de 2023).

Cluzel, François Du. 2021. "Cognitive Warfare, A Battle For The Brain." In Cognitive Warfare: The Future of Cognitive Dominance, edited by Bernard Claverie, Baptiste Prébot, Norbou Buchler e François du Cluzel. First NATO Scientific Meeting on Cognitive Warfare. www.innovationhub-act.org/sites/default/files/2022-03/Cognitive%20Warfare%20Symposium%20-%20ENSC%20-%20March%202022%20Publication.pdf (Acesso em 04 de agosto de 2023).

Cordey, Sean. 2019. "Cyber Influence Operations: An Overview and Comparative Analysis." *Center for Security Studies*. http://hdl.handle.net/20.500.11850/382358 (Acesso em 20 setembro 2023).

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

Derleth, James. 2021. "Russian New Generation Warfare." *Military Review* 100, no.5 (Sep/Oct 2020): 82-94

Diniz, Eugenio. 2024. "Uma Análise Preliminar Do Ambiente Informacional Contemporâneo No Brasil." *Análise Estratégica* 32, no.1: 59-75.

Duarte, Érico Esteves. 2020. *Estudos estratégicos*. Curitiba: InterSaberes.

Estados Unidos. 1996. *Field Manual (FM) 100-6, Information Operations*. https://www.hsdl.org/?view&did=437397 (Acesso em 24 de junho de 2024).

Estados Unidos. 2016. *Field Manual (FM) 3-13 Information Operations December 2016*. https://irp.fas.org/doddir/army/fm3-0.pdf (Acesso em 17 de junho de 2024).

Estados Unidos. 2022. *Field Manual (FM) 3-0 Operations October 2022*. https://www.globalsecurity.org/military/library/policy/army/fm/3-13/fm3-13_2016.pdf (Acesso em 17 de junho de 2024).

Frenkel, Sheera. 2024. "Israel Secretly Targets U.S. Lawmakers With Influence Campaign on Gaza War." New York Times. https://www.nytimes.com/2024/06/05/technology/israel-campaign-gaza-social-media.html (Acesso em 17 de junho de 2024).

Giordano, James. 2017a. "Neuroscience in irregular warfare." Newport: Invited plenary: Center for Irregular Warfare and Groups, US Naval War College.

Giordano, James. 2017b. "Neuroscience and neurotechnology as leverage for strategically latent influence upon the 21st century global stage". Maryland: Plenary Session: Joint Base Andrews, MD: SMA Strategic Influence Conference.

Giordano, James. 2017c. "Neuroscience and technology as weapons on the twenty-first century world stage." *In Influence in an Age of Increasing Connectedness*, edited by W. Aviles and S. Canna, 58-66. Department of Defense: Strategic Multilayer Assessment Group-Joint Staff/J-3/Pentagon Strategic Studies Group.

Giordano, James. 2021. "Emerging Neuroscience and Technology (NeuroS/T): Current and Near Term Risks and Threats to Nato Biosecurity." *NATO Innovation Hub*: 24–35. https://www.innovationhub-act.org/sites/default/files/2021-03/NATO%20NeuroST%20Report%20FINAL.pdf (Acesso em 17 de abril de 2023).

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

Green, James. 2015. *Cyber Warfare: A Multidisciplinary Analysis*. London: Routledge.

Houghton, David Patrick. 2009. Political Psychology: Situations, Individuals and Cases. New York: Routledge.

Heuer, Richards. 1999. *Psychology of intelligence analysis*. Center for the Study of Intelligence.

Hoffman, Frank. 2018. "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges". *PRISM* 7, no.4: 31-47.

Huhtinen, Aki-Mauri. 2007. "Different types of information warfare." In *Electronic Government: Concepts, Methodologies, Tools, and Applications*, edited by Ari-Veikko Anttiroiko, 310-314. Tampere, Finland: University of Tampere Press.

Jaccard, James e Jacob Jacoby. 2010. *Theory Construction and Model-Building Skills: a practical guide for social scientists*. New York: The Guilford Press.

Japão. 2022a. *National Security Strategy of Japan*. Tóquio: National Security Council and Cabinet meeting. https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf (Acesso em 4 de setembro de 2024).

Japão. 2022b. *National Defense Strategy*. Tóquio: Ministério da Defesa. https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy_en.pdf (Acesso em 04 de setembro de 2024).

Johnson, Adam e Othman Ali. 2024. "Coverage of Gaza war in the New York Times and other newspapers heavily favored Israel, analysis shows". *The Intercept*. 09 de janeiro de 2024. https://theintercept.com/2024/01/09/newspapers-israel-palestine-bias-new-york-times/. (Acesso em 28 de novembro de 2024).

Jindal, Divyanshu. 2023. "India in the Age of Cognitive Warfare." India Foundation. https://indiafoundation.in/wp-content/uploads/2023/09/Divyanshu-Jindal-combined-Final-48-pages.pdf (Acesso em 04 de setembro de 2024).

Kahneman, Daniel, Paul Slovic and Amos Tversky. 1982. *Judgment under uncertainty: Heuristics and biases*. Cambridge: Cambridge University Press.

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

Kahneman, Daniel. 2011. *Fast and slow thinking*. New York: Allen Lane and Penguin Books.

Keman, Hans, Jan Kleinnijeh e Paul Pennings. *Doing Reserach in Political Science*. Sage, 2003.

Knyazev, Norman and Harrie Oosterhuis. 2022. "The bandwagon effect: not just another bias." In *Proceedings of the 2022 ACM SIGIR International Conference on Theory of Information Retrieval*, edited by Fabio Crestani, Gabriella Pasi and Eric Gaussier, 243-253. New York: Association for Computing Machinery.

Kuehl, Daniel. 2009. "From Cyberspace to Cyberpower: Defining the Problem." In Cyberpower and National Security, edited by Franklin D. Kramer, Stuart Starr and Larry K. Wentz, 26–28. Washington, DC: National Defense University Press.

Lauterbach, Claire e Namir Shabibi.2023. "Analysis: how the UK and US Media dehumanise palestinians" *Declassified UK*, 22 de novembro de 2023. https://www.declassifieduk.org/analysis-how-the-uk-and-us-media-dehumanise-palestinians/ (Acesso em 28 de novembro de 2024).

Lauterbach, Claire e Namir Shabibi.2024. "Leaked Documents show pro-Israel bias at major newswire" *Declassified UK*, 07 de fevereiro de 2024. https://www.declassifieduk.org/leaked-documents-show-pro-israel-bias-at-major-newswire/ (Acesso em 28 de novembro de 2024).

Maschmeyer, Lennart, Alexei Abrahams, Peter Pomerantsev and Volodymyr Yermolenko. 2023. "Donetsk Don't Tell – 'Hybrid War' in Ukraine and the Limits of Social Media Influence Operations." *Journal of Information Technology & Politics* (May): 1–16. doi:10.1080/19331681.2023.2211969.

Mccreight, Robert. 2022. "Neuro-cognitive Warfare: Inflicting Strategic Impact via Non-Kinetic Threat." *Small Wars Journal*. https://smallwarsjournal.com/jrnl/art/neuro-cognitive-warfare-inflicting-strategic-impact-non-kinetic-threat (Acesso em 18 de abril de 2023).

McGreal, Chris. 2024. "CNN staff say network's pro-Israel slant amounts to 'journalistic malpractice'. *The Guardian*. 04 de fevereiro de 2024. https://www.theguardian.com/media/2024/feb/04/cnn-staff-pro-israel-bias. (Acesso em 28 de novembro de 2024)

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

Neto, Ricardo Borges Gama. 2017. "Guerra Cibernética/Guerra Eletrónica-Conceitos, Desafios e espaços de interação." *Revista Política Hoje* 26, no. 1: 201-217.

Paikowsky, Deganit, e Evitar Matania. 2019. "Influence Operations in Cyber: Characteristics and Insights." In *The Cognitive Campaign: Strategic and intelligence Perspectives*, edited by Yossi Kuperwasser and David Siman-Tov. Institute for National Security Studies. https://www.inss.org.il/wp-content/uploads/2019/10/Memo197_e_compressed.pdf

Pamment, James, Howard Nothhaft, Alicia Fjällhed and Henrik Agardh-Twetman. 2018. *Countering information influence activities: The state of the art*. https://rib.msb.se/filer/pdf/28697.pdf (Acesso em 17 de junho de 2024).

Paul, Katie. 2023. "Meta pins pro-China influence campaign on Chinese law enforcement." *Reuters*, 30 de agosto de 2023. Nova York. https://www.reuters.com/technology/meta-pins-spamouflage-influence-campaign-chinese-law-enforcement-2023-08-29/ (Acesso em 17 de junho de 2024).

Pocheptosov, Georgy. 2016. "Five New Trends in the Transformation of the Information War: Future Approaches." https://psyfactor.org/psyops/infowar47-2.html (Acesso em 02 de abril de 2020).

Psychological Defence Agency. 2024. https://mpf.se/psychological-defence-agency (Acesso em 04 de setembro 2024).

Schmitt-Beck, Rüdiger. 2015. *Bandwagon Effect: In the International Encyclopedia of Political Communication*. Hoboken, NJ: John Wiley & Sons. https://doi.org/10.1002/9781118541555.wbiepc015

Schmidt-Felzmann, Anke. 2017. "More than 'just' Disinformation. Russia's Information Operations in the Nordic Region." In *Information Warfare. New Security Challenge for Europe*, edited by Tomas Cizik, 32-67. Bratislava: Centre for European and North Atlantic Affairs.

Stiennon, Richard 2015. "A short history of cyber warfare." In *Cyber Warfare: A Multidisciplinary Analysis*, edited by James Green, 7-32. London: Routledge.

Takagi, Koichiro 2022. "The Future of China's Cognitive Warfare: Lessons from the War in Ukraine." War on the Rocks. https://warontherocks.com/2022/07/the-future-of-chinas-cognitive-warfare-lessons-from-the-war-in-ukraine/ (Acesso em 22 de julho de 2022).

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.252
ISSN 2595-4717

Walker, Márcio. 2024. *Operações de informação: névoa de conceitos*. Maringá: Viseu.

Walton, Calder. 2019. "Spies, Election Meddling and Disinformation: Past and Present." *Brown Journal of World Affairs* 26 (Fall/Winter 2019), no.1: 107-124.

Wanless, Alicia, and James Pamment. 2019. "How do you define a problem like influence?." *Journal of Information Warfare* 18, no. 3: 1-14.

Passage, David. 2009. "Reflections on psychological operations: the imperative of engaging a conflicted population." In *Ideas as Weapons: Influence and Perception in Modern Warfare*, 49-58, edited by T. R. Mckeldin III and G. J. David Jr. Virginia: Potomac Books.

Paul, Christopher. 2011. *Strategic communication: origins, concepts, and current debates*. Santa Barbara; Denver; Oxford: Praeger.

Snyder, Alvin. 1995. *Warriors of disinformation: how lies, videotape, and the USIA won the cold war*. New York: Arcade Publishing.

Shulsky, Abram. 2002. "Elements of strategic denial and deception." In *Strategic Denial and Deception: The Twenty-First Century Challenge*, edited by James Wirtz and Roy Godson. New Brunswick, Londres: Transaction publishers.

Whaley, Barton. 2007. *Deception and surprise in War*. Boston, Londres: Artech House.

Yun, Minwoo e Eunyoung Kim. 2022. "Cyber Cognitive Warfare as an Emerging New War Domain and Its Strategies and Tactics." *The Korean Journal of Defense Analysis* 34, no.4: 603–31. www.scholarworks.bwise.kr/gachon/handle/2020.sw.gachon/86763.