O Poder Invisível das Autocracias: Guerra Cognitiva

Roberto Narciso Andrade Fernandes[1]

Resumo

Este artigo examina a guerra cognitiva como elemento central da competição estratégica global, com foco nas operações informacionais da Rússia e da China. Defende-se que estas potências combinam guerra híbrida, cognitiva e de influência para estruturar redes de disrupção que visam corroer a confiança social, manipular perceções e enfraquecer democracias. A análise sublinha que a emergência da inteligência artificial generativa inaugura uma nova etapa da guerra da informação, marcada pela escalada da manipulação epistémica, cujo impacto pode rivalizar com a violência material. As operações sino-russas são interpretadas como catalisadores da fragmentação da ordem internacional, ampliando riscos tecnológicos, políticos e societais. Conclui-se pela urgência de uma resposta

[1] Doutor em Relações Internacionais, especializado em Geopolítica e Geoeconomia. Superintendente da Polícia de Segurança Pública. Coordenador do Curso de Pós-Graduação em Comando e Estratégia Policial no Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI). Membro do Conselho Editorial do CEPOL European Law Enforcement Research Bulletin (2023–2025) e colabora como perito externo para a CEPOL e a COST. Anteriormente, dirigiu o Centro de Investigação ICPOL (2019-2023), em Lisboa; chefiou a Área Operacional da Polícia de Segurança Pública, na Madeira (2023-2024).

multidimensional, baseada na resiliência cognitiva, na literacia mediática e na cooperação estratégica entre democracias, como condição para a defesa da estabilidade global.

Palavras-chave: China, desinformação, geopolítica, guerra cognitiva, Rússia.

Abstract

This article examines cognitive warfare as a central element of contemporary strategic competition, focusing on the informational operations conducted by Russia and China. It argues that these powers integrate hybrid, cognitive, and influence warfare to build disruption networks aimed at eroding public trust, manipulating perceptions, and weakening democratic institutions. The analysis highlights how the emergence of generative artificial intelligence marks a qualitatively new stage in the information battlespace, where epistemic manipulation may prove as disruptive as material violence. Sino-Russian influence operations are interpreted as catalysts of international fragmentation, amplifying technological, political, and societal risks. The article concludes by stressing the urgency of a multidimensional response, centred on cognitive resilience, media literacy, and strategic cooperation among democracies, as essential conditions for safeguarding global stability.

Keywords: China, cognitive warfare, disinformation, geopolitics, Russia.

Introdução

Divulgado em 1977, *Rocket to Russia*, o álbum de originais da mítica banda norte-americana Ramones, destacou-se como uma das obras emblemáticas do punk rock, influenciando gerações. Espelhando o clima de desconfiança, paranoia e absurdidade política da época, o valor simbólico e despretensioso da obra reconduz-nos ao tenso ambiente de confrontação geopolítica entre as democracias ocidentais e a Rússia, numa altura em que o Kremlin voltou a assumir um papel beligerante na cena internacional, como evidenciado pela invasão militar da Ucrânia, em 24 de fevereiro de 2022, num conflito prolongado e que estende até aos dias de hoje (Galeotti, 2022; Applebaum, 2024). De acordo com Steve Killelea, fundador e presidente executivo do Instituto para a Economia e Paz (IEP), o conceito de "guerras intermináveis" é mais real do que nunca. A fragmentação global está a acelerar a ritmo alucinante, sinalizando um potencial ponto de viragem para uma nova ordem internacional (Schuman, Fulton, & Gering, 2023; *Institute for Economics & Peace*, 2025).

O reacendimento do confronto dos blocos Este-Oeste e da lógica da corrida armamentista ao estilo de uma "guerra fria 2.0", evoca a ameaça mútua de aniquilação num momento em que a possibilidade de uma querela nuclear volta a ser parte do quotidiano imaginário ocidental, ganhando densidade em toda a União Europeia (UE), agora apostada em se rearmar (Brands & Gaddis, 2021). O plano de resiliência europeu – "Prontidão 2030" – visa aumentar as capacidades de defesa militar e a produção armamentista em todo o flanco ocidental, tendo por horizonte o guarnecimento logístico da UE antes da data em que se estima que a Rússia terá as capacidades bélicas necessárias para lançar um ataque contra um Estado-membro da UE ou da Organização do Tratado do Atlântico Norte (OTAN/NATO). Segundo o ex-Chefe do Estado-Maior do Exército

britânico, general Patrick Sanders, os sinais da ameaça russa são por demais evidentes, sendo que a ocorrência de um confronto militar é, cada vez mais, uma possibilidade realística. "Se a Rússia parar de combater na Ucrânia, chegamos a uma situação em que, num espaço de poucos meses, ela terá capacidade para lançar um ataque limitado contra um membro da NATO, o que nos obrigará a intervir, e isso poderá acontecer até 2030" (Patrick Sanders *apud* Sheridan D., 2025). Este receio antigo – da Rússia poder "chegar com os tanques à praça da Concórdia" (Costa, 2025) – é corroborado pelo Chefe do Estado-Maior das Forças Armadas francesas, general Thierry Burkhard, que sustenta que a Federação Russa representa uma ameaça imediata e persistente, encarando o conflito na Ucrânia como uma questão existencial. Segundo a responsável pela contrainteligência alemã, Martina Rosenberg, as operações encobertas russas na Alemanha, enquanto centro logístico para os movimentos de tropas da OTAN e parceiro ativo da Aliança, têm vindo a crescer exponencialmente e de forma mais agressiva. "(…) Estamos a falar de um aumento acentuado dos casos de espionagem e de medidas híbridas (…)" (Rosenberg *apud* Verhelst, 2025). Para o presidente ucraniano, Volodymyr Zelensky, "(…) não é apenas especulação ociosa; a ameaça é real. O objetivo final de Putin é reviver o império russo e recuperar territórios atualmente sob proteção da OTAN" (Zelenskyy, 2025).

Nesta conjunção belicosa, o regime russo – entretanto, declarado como um Estado patrocinador do terrorismo, à luz da Resolução P9_TA (2022)0405, aprovada em 23 de novembro de 2022, pelo Parlamento Europeu – persiste determinado em exaurir a Europa, capturar o território ucraniano e em desmantelar a OTAN (Dugin, 1997; Cláudio, 2015; Sahuquillo, 2024; Fernandes, 2025; Vincent, 2025; Zakaria, 2025). A escalada da tensão é alimentada pelas declarações do presidente do Conselho de Segurança da Rússia, Dmitry Medvedev, o qual defende, de viva voz, que a Rússia deve estar

pronta para atacar o Ocidente se este escalar a guerra na Ucrânia (Reyes, 2025). Referindo-se à crescente militarização e ao sentimento de confrontação europeu, o porta-voz do Kremlin, Dmitry Peskov,afirmou "(…) estamos muito desiludidos por os sinais absolutamente claros e consistentes que estão a ser enviados de Moscovo (…) não estarem a ser tidos em conta, nem a ser compreendidos" (Aktas, 2025). Atenda-se que, paradoxalmente, a Rússia, ao invadir a Ucrânia, estimulou a adesão da Finlândia e da Suécia à Aliança Atlântica, algo impensável durante décadas, especialmente por causa das tradições de neutralidade militar daqueles Estados nórdicos, profundamente enraizadas em suas histórias, sociedades e políticas externas. Consequentemente, vários estudiosos, analistas geopolíticos e ex-diplomatas argumentam que esta guerra contra a Ucrânia foi um erro crasso do presidente Vladimir Vladimirovitch Putin, cujas consequências negativas, para além do engrossar dos Estados-membros da OTAN, incluem o isolamento internacional da Rússia, o enfraquecimento económico interno, o fortalecimento do sentimento nacionalista ucraniano e a perda de influência geopolítica no cenário global (Freedman, 2015; Hill & Gaddy, 2015; Kofman, Migacheva, Nichiporuk, Radin, & Oberholtzer, 2017; Bremmer, 2018; Snyder, 2022; Applebaum, 2024).

No final da década de 1970, as democracias ocidentais enfrentavam uma crise múltipla, marcada por forte instabilidade económica, desconfiança nas instituições políticas e uma crescente contestação social. A estagflação, agravada pelos choques no sistema petrolífero de 1973 e 1979, comprometeu o crescimento e alimentou o desemprego, enquanto escândalos como o tristemente famoso caso *Watergate*, nos Estados Unidos da América (EUA), conduziram à saída forçada do presidente Richard Nixon e minaram, de modo geral, a legitimidade dos regimes democráticos. Simultaneamente, o aumento da violência político-ideológica, com a atuação de grupos terroristas como as *Brigate Rosse*, em Itália, e a *Rote Armee Fraktion*, na Alemanha

Ocidental, evidenciava a radicalização de sectores da sociedade desiludidos com o sistema vigente. A par disso, movimentos sociais emergentes, como o feminismo e o ambientalismo, desafiavam as normas estabelecidas, contribuindo para um clima de polarização e incerteza quanto ao futuro do modelo democrático liberal. Esta conjuntura tensionada abriu espaço fértil para manifestações de contestação em várias frentes, nomeadamente nos planos político e cultural (Hobsbawm, 1995; Hebdige, 2013).

Quase cinco décadas depois, o mundo vivencia novas criticidades existenciais em razão da política internacional de blocos. Depois de uma pandemia (Covid-19) que suspendeu o mundo e nos apresentou ao "novo normal", a invasão militar russa à Ucrânia, em 2022, marcou o regresso da guerra – mas, desta feita, de traço não convencional, híbrido e prolongado – a um continente europeu envelhecido, pacifista e desarmado, renovando os vigores expansionistas do legado soviético, perante a indiferença republicana dos EUA[2] e a passividade de uma Europa unificada, mas enfraquecida por "cavalos de tróia" húngaros e eslovacos (Giles, 2016; Verhelst, 2025). Afirmando-se como uma potência revisionista de propósito imperial, a Rússia desafia, presentemente, os equilíbrios construídos no pós-Segunda Guerra Mundial (1939-1945) e no período de otimismo democrático que sucedeu à dissolução da União Soviética, em 1991, com a firme resolução de implementar uma nova ordem mundial de perfil multipolar e euroasiático (Dugin, 1997 e 2025; Sakwa, 2021). Na verdade, a antiga União Soviética de Josef Stálin,

[2] Apesar da inflexão da política externa norte-americana e da ambiguidade latente da administração Trump, os EUA ainda fazem parte da Aliança Ocidental no sentido institucional. A política externa americana revela-se menos previsível, mais transacional e menos comprometida com os valores democráticos que unificaram o Ocidente desde a Segunda Guerra Mundial. Estes sinais anunciam uma nova doutrina americana, na qual o país não abandona o Ocidente, mas deixa de liderá-lo. O unilateralismo, o transacionalismo e o ceticismo de Trump em relação às democracias liberais aprofundam a divisão do Ocidente e potenciam o fortalecimento da Rússia e da China enquanto atores globais.

Nikita Khrushchov ou Leonid Brejnev e a moderna Rússia de Vladimir Putin partilham denominadores comuns contra o Ocidente plural, como a ameaça velada, a opacidade do poder e a disposição para o uso da força (*hard power* em detrimento do *soft power*[3]) em nome de um ideal irredentista (Duranty, 1944; Wilson, 2008; Wood, 2013; Kissinger, 2014; Nye, 2008 e 2023). Se, na década de 1970, o regime russo era delineado pelos média e pela propaganda comunista, hoje ele ressurge através de ações beligerantes consistentes, como a anexação da Crimeia ucraniana (2014) e a referida invasão à escala total da Ucrânia (2022); a guerra híbrida, incluindo as chamadas "operações de influência" e a desinformação [4]; espionagem [5] e sabotagem internacional; bem como o apoio a movimentos nacionalistas antiocidentais; entre outras exteriorizações mavórcias (Bayer, *et al*., 2021; NATO | OTAN, 2024). Que não persistam dúvidas: desde 2014, a Rússia declarou guerra aberta ao Ocidente e ao internacionalismo liberal (Olszański, Sarna, & Wierzbowska-Miazga, 2014; Giles, 2016; Sobchuk, 2025; Todd, 2025).

---

[3] O *soft power* (ou "poder brando") é a capacidade de influenciar outros atores de modo a alcançar os resultados desejados, recorrendo à atração em vez da coerção ou do pagamento. O *soft power* de um país assenta nos seus recursos culturais, nos valores que professa e nas políticas que adota. Uma estratégia de *smart power* ("poder inteligente") combina recursos de *hard power* (poder coercivo) com os de *soft power*, articulando-os de forma estratégica. A diplomacia pública tem uma longa tradição enquanto instrumento de promoção do *soft power* de um Estado, tendo desempenhado um papel fulcral na vitória da guerra fria. No contexto atual, marcado pela luta contra o terrorismo transnacional, trata-se sobretudo de conquistar corações e mentes, mormente quando a dependência excessiva do poder coercivo não se revela, por si só, uma via eficaz para o sucesso. A diplomacia pública constitui, assim, uma ferramenta essencial no arsenal do *smart power*. No entanto, uma diplomacia pública verdadeiramente eficaz exige um entendimento profundo do papel da credibilidade, da autocrítica e da sociedade civil na geração de *soft power* (Nye, 2008 e 2023; Walker & Ludwig, 2017).

[4] Em 2024, a desinformação e a informação falsa constituíram os maiores riscos a curto prazo, enquanto os fenómenos climáticos extremos e as alterações críticas nos sistemas terrestres foram as maiores preocupações a longo prazo (*World Economic Forum*, 2024).

[5] A título exemplificativo, em julho de 2025, os serviços de inteligência britânicos identificaram 18 espiões russos envolvidos em atos de sabotagem no Reino Unido (Barnes, Kelly, & Mendick, 2025)

Neste contexto de conflitualidade, concorrência, competição e afirmação pela força no palco mundial, centenas de mísseis russos e enxames de drones *Shaheds*, fornecidos por vários regimes autocráticos, têm fustigado indiscriminadamente infraestruturas civis, escolas e hospitais por toda a Ucrânia, relembrando a comunidade internacional que a *Realpolitik* e a lógica de confrontação armada estão de volta e que não são relíquias de um passado distante (Galeotti, 2022; Applebaum, 2024). Na verdade, o "Eixo dos Autoritários" (composto pela Rússia, Bielorrússia, China, Irão, Coreia do Norte, Laos e Síria) digladia-se abertamente contra a Aliança Ocidental (constituída pela UE, Reino Unido, EUA – apesar retraídos pela dinâmica transacional e nebulosa de Mar-a-Lago –, Canadá, Austrália, Japão, Coreia do Sul e OTAN), quer no teatro ucraniano (com apoio armamentista, logístico e operacional), quer no plano comercial, económico, diplomático, político, ideológico, informacional, cibernético e outros (Lake, Martin, & Risse, 2021; Applebaum, 2024; Dugin, 2025; Alexandre, 2025).

As operações de influência dos principais regimes autocráticos, nomeadamente o chinês e o russo, cadenciam uma investida invisível e multidimensional contra o liberalismo democrático ocidental, com o objetivo de o reduzir a cinzas e edificar um novo sistema internacional, multipolar e de centralidade euroasiática, também chamada por *post Western order* (Dugin, 2025). A Europa é o alvo primário das ofensivas de manipulação e interferência estrangeira na informação[6], designadamente por parte da Rússia, sob o olhar atento da China, a grande arquiteta da geopolítica de confrontação. Em 2024, os incidentes analisados pelo Serviço de Ação Externa da UE (SEAE) apontam que as operações de

[6] *Foreign information manipulations and interference* (FIMI).

influência e desinformação russas focaram maioritariamente a Ucrânia (37,4%), França (21,2%), Alemanha (8,1%), Espanha (4,0%), Polónia (3,5%) e Bélgica (3.0%). Depois da Europa, a zona africana do Sahel destaca-se com 18,2% de incidência (Kruttke, 2024; Moysan, 2025). O perfil caleidoscópico e não-convencional do conflito híbrido contemporâneo, marcado pela fluidez dos meios, pela diversidade e informalidade dos agentes e pela incerteza dos alvos, distendeu o campo de batalha aos domínios do digital, da (des)informação, da cognição e da perceção (Verhelst, 2025). A confrontação geopolítica moderna não se limita ao uso isolado da força militar, incorporando uma dimensão informacional altamente sofisticada, onde a manipulação da narrativa pública, o controlo da memória coletiva e a criação de ambiguidade (*fake news* e "factos alternativos") são utilizados como armas de desestabilização sistémica (Fernandes, 2025). O dinamismo destas operações de influência antiliberais espelha, frequentemente, uma simbiose estratégica que alia a experiência russa em guerra psicológica com o alcance tecnológico e o aparato comunicacional chinês (Sheridan M., 2025).

Uma recente investigação oficial francesa identificou múltiplas vagas de campanhas de desinformação de dimensão e alcance sem precedentes, atribuída a círculos pró-Kremlin e que tem visado a França. Esta portentosa operação híbrida, coordenada entre diferentes entidades, como o Portal *Kombat* (ou rede *Pravda*) e a *Social Design Agency* (SDA), destinava-se a polarizar a sociedade francesa e enfraquecer o seu apoio à Ucrânia (Tril, 2025). Combinando ferramentas privadas, canais oficiais e manipulação de algoritmos para garantir visibilidade consistentes, entre janeiro e abril de 2025, as cinco principais notícias falsas tiveram 55 milhões de visualizações. Todos estes formatos são distribuídos massivamente através de redes de *bots*, *trollfarms*, *hactivistas* e hackers de aluguer, grupos inativos em plataformas sociais, contas online ou sites de imprensa clonados,

comprovando que a desinformação já não é apenas "ruído de fundo", mas uma variável estratégica permanente com assinalável capacidade de penetração disruptiva [7] (Dukach, Adam, & Furbish, 2025). A

[7] Uma investigação do *Atlantic Council* desmantelou uma enorme rede de *trolls* e *bots* associada a operações de influência e manipulação de informação pró-russa, na medida em que nenhuma delas corresponde a pessoas reais. Passamos a referir 136 contas e *usernames* com maior atividade *online*: *xierdymeabe, uminagrn, padraysherta, rearaiaquqta, sasasinsaniahe, wodenigal, hanowledalebeh, shashagerphini, breytelindett, vamikenand, ishieonand, qugghristtehh, yalaundri, galoorso, juragat, zarisichiridlin, onyerlannetyo, tuenaded, xwieloinko, qusinaroor, chunderoneko, ftvackenne, querlassh, mabrelldaraymi, ggikonanashah, konalenaloke, ananxionlion, chanureole, wiansyet, chuddeldadarios, onreroleth, quprenetu, sherootloataann, mckenzie020717, zylilasha, manionbieyrd, pieglala, xileveearadit, kewelian, yalishka, qiekasthelab, ubsashdal, lakyaleyebyo, qlaylowindnoo, hunleveadihass, orartonnerla, falloldannea, zavyinsyth, nierlartalo, retleflaet, qdutynenaf, ulanoneweth, ubashdal, gionedoraloll, warserapanhta, shokailudar, yorysthakar, yanaillithe, enchaheeridir, vreelinet, stelonoc, jaymaniosank, quinilemina, cinoton, bananuneoana, narlonlea, wartinandi, waytaronnansh, davlonsanard, wieranamchhh, dallareroraru, alvjasocondety, tinanleck, oisiarhargi, micrionlare, farindevaona, xaniylnasota, reashaletlely, vvp_gruater, emarvansorqu, nerfelarlat, nerlartalo, lakyaleyebyo, huanguanyueyinq, belazaycomenian, keloreda, freetolasar, mehdovia, dakadenger, hiraajaristy, diyurian, hajarriisty, emepafat, zlisconabile, gdrdoylome, groylome, nnenhelim, peydona, ffanontieri, eleganttinda, tarsarno, sheralothataan, qlaylowindnoo, uaiceeol, tanoleasha, stalaivahieftat, ghedvediavy, yananddenka, freinch_happiness_uee, magomed_nuraev, xinveronanka, qdutynenaf, tubnin, kxiakoaxi, nidarinowk, brielotedd, traymannas, ranveriyaraslay, soloralavoh, squedinorar, qurarienneneoo, gelsainetr, warserapanhta, bamiahamesno, zenokedetttt, oxirasihargi, ymatyptgy3y, yetcatcyiko, osiarhargi, qtiancharvarsti, wessonordiclule, tlianberwhosenn, envararvansorqu, vinoninayynn, erieronces, ashoronas, vsibahshtar, reebhace, vanoniaranas, falldonlanene, waerliachou, bribilinaeia, umniyayoungli, tianledaowy, rtelonasnor, uanabioch, yonickach, n_u111, dishollie, misekima, nellenota, gdroyolome, yanankok, jinleach, qdutynenaf, yanasibngmai, yanshhemngai, yteudondotneh, hunlevadiassh, qluayedveasi, moneisnoq, orassedda, anreryanir, anreranytir, treesezail, gohenolu, ginoridl, vellebierar, elegantrinsht, jeltannnni, frairannanh, yartorloth, yertorletth, yertorletet, maksim_solncevv* (Dukach, Adam, & Furbish, 2025). Ainda recentemente, a *Google* anunciou a remoção de quase 11.000 canais do *YouTube* coordenados por diferentes entidades e Estados, na maioria ligados à Rússia e à China, associados a campanhas de desinformação e propaganda sino-russas. A *Meta*, empresa-mãe do *Facebook* e do *Instagram*, anunciou recentemente a remoção de dez milhões de contas falsas durante o primeiro semestre de 2025, no âmbito de uma operação orientada para o combate a conteúdos automatizados e redes de desinformação. As revelações ocorrem num momento de maior escrutínio global sobre o impacto das grandes plataformas digitais na propagação de propaganda e na proteção da integridade informativa em contextos geopolíticos tensos (Agência Lusa, 2025b).

censura pelo ruído é uma realidade incontornável da confrontação geopolítica do século XXI (Agência Lusa, 2025a; Fernandes, 2025).

1.1. Problema de Investigação e Metodologia

Buscando explicitar como é que as operações de influência da Rússia e da China estão a reconfigurar os equilíbrios de poder mundial, a presente investigação recorreu a uma revisão bibliográfica criteriosa, tendo em vista assegurar rigor e relevância no domínio da guerra cognitiva e da informação (Backes & Swab, 2019). Nesse sentido, considerou-se apenas os estudos produzidos, a partir de 2018, por parte de instituições amplamente reconhecidas em Estudos de Segurança e Relações Internacionais – designadamente *Royal United Services Institute for Defence and Security Studies* (RUSI), *Institute for the Study of War* (ISW), *World Economic Forum* (WEF), NATO *StratCom Centre* e *EUvsDisinfo* –, de modo a abarcar os contributos mais recentes deste campo do Saber. Adicionalmente, privilegiou-se a diversidade geográfica das análises, contemplando perspetivas russas, chinesas e ocidentais, bem como a existência de dados empíricos consistentes, tais como estatísticas de plataformas digitais, mapeamento de redes de desinformação e estudos de caso *in loco*. Outrossim, favoreceram-se estudos e relatórios cujos autores comprovassem, de forma transparente, os procedimentos metodológicos prosseguidos, nomeadamente as amostras e instrumentos de recolha para consequente validação científica.

O processo de estudo organizou-se em três fases principais. Em primeiro lugar, procedeu-se ao levantamento inicial em bases académicas (*Scopus*, *Web of Science*) e nos repositórios oficiais dos referidos *think tanks*. Seguiu-se uma triagem dos títulos e resumos para aferir o alinhamento com as palavras-chave centrais da

investigação, após a qual se fez a leitura integral dos textos pré-selecionados, extraindo-se informação relativa ao ano de publicação, objetivos de investigação, metodologia empregue e principais conclusões. Perfilhámos ainda uma análise de conteúdo para categorizar temas recorrentes, construindo-se uma matriz de codificação em que cada conceito relevante foi registado, segundo uma lógica binária, em cada documento. Paralelamente, identificaram-se estudos de caso emblemáticos – como a campanha *Spamouflage*[8], de 2022, e as alegadas interferências estrangeiras em processos eleitorais europeus (Reino Unido em 2016 (*Brexit*); França e Alemanha em 2017; Suécia em 2018; Parlamento Europeu em 2019; Itália e Espanha em 2023) e norte-americanos (2016, 2018 e 2020) – procedendo-se ao seu mapeamento cronológico, à identificação dos fatores-chave, à análise dos canais de difusão (*e.g.* aplicações e redes sociais) e à avaliação dos seus impactos. Finalmente, recorreu-se à triangulação de fontes, confrontando dados secundários, tais como relatórios institucionais e estatísticas de plataformas, com literatura académica e artigos jornalísticos especializados, de modo a considerar apenas evidências confirmadas por fontes independentes (Patton, 2002).

[8] A campanha *Spamouflage*, também conhecida por *Dragonbridge*, *Spamouflage Dragon*, *Storm 1376* ou *Taizi Flood*, foi uma operação de influência (propaganda e desinformação) atribuída ao governo chinês, voltada à promoção de narrativas pró-China e à desinformação em escala global. Utilizando redes de contas falsas em plataformas como *Facebook*, X (*Twitter*), *YouTube*, *TikTok* e *Reddit*, o grupo disseminava conteúdos repetitivos, muitas vezes com traduções automatizadas, para atacar críticos do regime chinês e promover temas polémicos, como a legitimidade do governo chinês em relação a Taiwan, Hong Kong e Xinjiang. A campanha também visava desacreditar rivais geopolíticos como os EUA, Japão e Índia, além de tentar influenciar eleições e manipular a opinião pública, fingindo possuir apoio popular local. A rede foi descoberta por empresas como *Meta*, *Google* e *Microsoft*, que tomaram medidas para derrubar milhares de contas e canais envolvidos. O nome "*Spamouflage*" é uma junção de "*spam*" e "*camouflage*", refletindo o uso massivo e disfarçado de propaganda digital (Bayer, *et al*., 2021; Meta, 2023; Bond, 2023; Bochantin, 2024).

Não obstante, reconhecem-se limitações ao estudo. A prevalência de documentos em inglês pode sub-representar contributos de outros especialistas pouco divulgados internacionalmente; a falta de acesso direto a bases de dados proprietárias das plataformas digitais impede uma análise quantitativa mais aprofundada; e o recorte temporal – até meados de 2025 –, exclui desenvolvimentos posteriores. Ainda assim, a transparência na seleção de fontes e a sistematização dos procedimentos metodológicos parecem-nos conferir solidez científica e a sua replicabilidade em estudos futuros.

Aclaramos que, no emolduramento geopolítico-concetual construído para a presente investigação, interpretaremos, doravante, a expressão "*rocket*" como o conjunto das ameaças híbridas sino-russas que tanto periclitam o modo de vida ocidental.

1.2. Objetivos e Contributo

Este estudo inova ao integrar numa única análise as dinâmicas sinergéticas das operações russo-chinesas de guerra cognitiva, articulando-as diretamente com um quadro sistemático de riscos globais e respostas de resiliência. Para além de consolidar conceitos dispersos na Ciência das Relações Internacionais, designadamente guerra híbrida, guerra cognitiva e operações de influência, a investigação introduz uma matriz de análise SWOT e propõe um Mapa de Riscos e Respostas, instrumentos inéditos considerados relevantes enquanto ferramentas analíticas e guias práticos para a formulação de políticas públicas e outras iniciativas de literacia e resiliência digital junto da sociedade civil. Desta forma, este trabalho contribui para o avanço teórico-metodológico do campo, oferecendo um modelo

replicável de análise e uma ponte entre a investigação académica e a ação política.

2. O Alcance e a Potência das Operações de Influência Sino-Russas

No prolongamento da conflitualidade coeva, as operações de influência sino-russas inscrevem-se no domínio "invisível" da guerra híbrida, enquanto instrumentos centrais de um novo tipo de confrontação geopolítica (*Intrisec*, 2025). Se, durante o período da chamada "guerra fria" (1947-1991), a propaganda soviética operava em moldes centralizados e previsíveis, presentemente, tanto a Rússia de Putin como a China de Xi Jinping recorrem a técnicas assimétricas, sofisticadas, opacas e adaptativas, desenhadas nos bastidores para subverter as democracias liberais a partir de dentro, diminuindo a confiança social e a coesão política (Duranty, 1944; Giles, 2016; Reagan, 2024; Sheridan M., 2025). A convergência de interesses disruptivos entre a Federação Russa e a República Popular da China neste domínio configura um fenómeno de elevada relevância geopolítica, caraterizado por uma crescente interdependência tática e estratégica (Hvistendahl & Kovalev, 2022; Boullenois, Kratz, & Rosen, 2025). Esta aliança geoestratégica transcende a mera partilha de interesses conjunturais, representando uma fusão operacional entre dois modelos autocráticos de guerrilha informacional e que conjuga, astuciosamente, a *infowar* e a *cyberwar* (Arquilla & Ronfeldt, 1993). A complexidade, caos e redundância epidémica vulnerabilizam o multilateralismo, baseado em regras e convenções, e as conceções tradicionais de segurança internacional (Salt & Sobchuk, 2021; Sobchuk, 2025).

O Estado russo, herdeiro direto das doutrinas soviéticas de medidas ativas e precursor da "diplomacia disruptiva", continua a ser

reconhecido como o principal catalisador de técnicas de rompimento, desinformação, instrumentalização da narrativa e controlo reflexivo, por forma a manipular os quadros mentais do público mundial em favor dos seus interesses imperialistas (Thomas, 2004; Ferreira & Terrenas, 2016; Giles, 2016). A eficácia desta estratégia infodémica dissimulada, baseada na subjugação do adversário através do caos provocado por quantidades massivas de dados desordenados e contraditórios, reside na sua capacidade de segmentar e distorcer a realidade discursiva, promovendo uma entropia informacional que constrange a confiança social e institucional (Pomerantsev, 2014; Polyakova & Meserole, 2019; Fernandes, 2025).

Por sua vez, a China tem vindo a abandonar progressivamente a sua postura mais reativa e reputacional nas esferas internacionais (Creemers, 2018). Através do realinhamento com as metodologias disruptivas moscovitas, Pequim adotou práticas de desinformação mais intrusivas e orientadas para a manipulação adaptativa de públicos estrangeiros, com recurso aos gigantes tecnológicos e conglomerados económicos. A campanha *Spamouflage*, que inicialmente se distinguia pelo seu conteúdo rudimentar e baixo alcance, rapidamente evoluiu para estratégias de disfarce ideológico como o "*MAGAflage*", onde se imita a retórica da direita populista norte-americana com o objetivo de infiltrar e amplificar tensões internas (*Institute for Strategic Dialogue*, 2024). Esta recalibração estratégica e operacional russo-chinesa em torno de uma *Lügenpolitik* ("política de mentiras") encontra expressão formal no acordo ministerial de cooperação mediática, assinado em 2021, que estipula a sincronização da narrativa, a partilha de conteúdos e a coordenação na esfera digital (Fernandes, 2025). A assinatura do acordo por representantes de colossos tecnológicos sugere uma crescente pronunciação entre infraestruturas tecnológicas e de propaganda

estratégica com o Eixo dos Autoritários, o que muito deve preocupar o ocidente democrático (Bayer, *et al*., 2021; Hvistendahl & Kovalev, 2022). Esta aliança institucional legitima a propagação concertada de narrativas distópicas, como a justificação da invasão russa à Ucrânia ou a deslegitimação do processo eleitoral em Taiwan, anunciando a emergência de um ecossistema informacional despótico de alcance global (Bochantin, 2024). A projeção opressiva e controladora proposta por George Orwell, na sua obra-prima "1984", é, hoje, uma realidade insofismável.

No plano utópico das democracias ocidentais, as operações *name and shame*, em especial as conduzidas por atores estatais como os EUA ou por agências da UE, assentam, em regra, numa lógica normativa de persuasão baseada em factos verificáveis, enquadrada por princípios democráticos e por um esforço de transparência comunicacional. A diplomacia pública norte-americana, através de organismos como o *Voice of America* ou o *USAGM*, procura projetar valores liberais e promover sociedades abertas, ainda que não seja isenta de críticas quanto à sua seletividade narrativa, em particular desde a subida de Trump ao poder na Casa Branca (Cull, 2009). A UE, por sua vez, desenvolveu instrumentos como o *EUvsDisinfo* e o *Rapid Alert System*, centrados na identificação, denúncia e refutação de desinformação dirigida ao espaço europeu (*European Court of Auditors*, 2020; Fernandes, 2025). Contudo, a resposta europeia continua a ser maioritariamente reativa, fragmentada e dependente da denúncia pós-facto, contrastando com a proatividade, intensidade e agilidade tática das operações sino-russas. A ausência de um quadro jurídico comum, as limitações orçamentais, bem como os diferentes níveis e tipos de ameaça – militar, nuclear, química, biológica, cibernética, tecnológica, informacional, híbrida, energética, económica, ambiental, espacial, etc. – percecionada entre Estados-

membros, comprometem a eficácia de uma estratégia concertada de defesa cognitiva (Hoffman, 2014; Bayer, *et al*., 2021; Fernandes, 2025). Acresce ainda que os regimes autoritários, ou "Autocracias, Inc.", como representados por Anne Applebaum, operam segundo uma lógica assimétrica e de *proxy*, onde a negação plausível e a densidade organizacional lhes permitem maior liberdade de ação e menor custo político (Applebaum, 2024). Enquanto o Ocidente privilegia a resposta institucional e legalista, as autocracias investem massivamente na manipulação emocional, cultural e identitária, explorando as fissuras internas das democracias liberais. A polarização política, a desconfiança institucional e a fragmentação mediática são as principais técnicas do Eixo dos Autoritários. Esta diferença estrutural de abordagem coloca os regimes democráticos em desvantagem ou, no mínimo, numa posição defensiva, exigindo uma revisão profunda dos instrumentos de resiliência cognitiva e da arquitetura de cibersegurança informacional (Darcy, *et al*., 2025).

3. Informação e Poder: A Centralidade da Guerra Informacional

A guerra informacional constitui-se, hoje, como um dos principais teatros de conflito nas relações internacionais, emergindo como um campo de batalha central no âmbito das estratégias de poder contemporâneas. Esta dimensão da guerra transcende os métodos tradicionais de combate, assumindo contornos multifacetados que englobam as noções de guerra híbrida, guerra cognitiva e guerra de influência (Backes & Swab, 2019).

O conceito de "guerra híbrida" refere-se à conjugação de meios convencionais e não convencionais, que combinam operações militares no terreno (*boots on the ground*) com táticas de desinformação, ciberataques, operações psicológicas e manipulação

mediática, entre outros (Hoffman, 2014; Gouliev, 2025). Assim, trata-se de uma forma de conflito que integra simultaneamente a violência física e a disputa simbólica, visando desestabilizar adversários sem recorrer exclusivamente à força bruta. Em paralelo, a "guerra cognitiva" incide sobre a perceção e a interpretação da realidade pelos indivíduos e coletividades, procurando moldar mentalidades e decisões através do controlo da informação e da construção de narrativas que alteram a perceção dos factos (Backes & Swab, 2019). Este tipo de guerra explora vulnerabilidades cognitivas, promovendo dúvidas, confusão e polarização, de modo a influenciar comportamentos e escolhas estratégicas (Backes & Swab, 2019, Fernandes, 2025). Por último, a "guerra de influência" abarca um conjunto de estratégias e técnicas destinadas a expandir o "poder suave" (*soft power*) de um ator, afetando a opinião pública, decisores políticos e atores sociais em várias esferas, com o objetivo de ganhar vantagem geopolítica e geoestratégica (Nye, 2008 e 2023). Nesta lógica, o domínio narrativo e simbólico torna-se crucial para garantir legitimidade e apoio em contextos de conflito ou competição internacional (Darcy, *et al*., 2025).

A Rússia emerge, no presente cenário, como um arquétipo da manipulação reflexiva na guerra informacional. O Estado russo tem desenvolvido um modelo sofisticado de influência que explora a ambiguidade e a desinformação, combinando ações diretas e indiretas para criar um ambiente de incerteza e dúvida (Giles, 2016). A sua estratégia assenta na capacidade de fomentar divisões internas nos países-alvo, explorar vulnerabilidades sociais e políticas, bem como utilizar meios digitais para amplificar discursos e mensagens desestabilizadoras. Esta manipulação reflexiva implica não apenas a propagação de informações falsas, mas também a utilização calculada da verdade parcial para gerar desconfiança e hesitação nos adversários (Pomerantsev, 2014 e 2017; Fernandes, 2025).

Paralelamente, a China tem vindo a evoluir um modelo próprio de guerra informacional, que inicialmente se centrava no controlo interno das informações para garantir a estabilidade política e social. Entre 2012 e 2014, os primeiros anos da liderança de Xi Jinping testemunharam uma reconfiguração profunda da governação da *internet* na China, com a criação de um quadro institucional centralizado destinado a integrar as tecnologias digitais nas estratégias de propaganda, controlo da opinião pública e vigilância social (Bayer, *et al*., 2021). Este processo implicou uma redução acentuada da autonomia do espaço digital, através do encerramento de canais de deliberação pública (Creemers, 2018). Contudo, mais recentemente, este modelo tem expandido o seu alcance para um âmbito global, caracterizado por um expansionismo narrativo que visa influenciar perceções internacionais e moldar a ordem comunicacional a seu favor (Brady, 2017). Através de uma combinação de censura, promoção de narrativas oficiais e investimento em meios de comunicação internacionais, a China procura consolidar a sua posição como ator global, não apenas através do poder económico e militar, mas também pelo controlo e difusão de discursos estratégicos que reforcem a sua legitimidade e objetivos geopolíticos (Shambaugh, 2007). Assim, a guerra informacional configura-se hoje como um campo central da disputa global, onde atores autocráticos exemplificam estratégias heterogéneas e muito sofisticadas, mas convergentes na sua aposta na manipulação da perceção e da narrativa como instrumentos decisivos de poder (Creemers, 2018; Darcy, *et al*., 2025).

4. Riscos Sistémicos e Estratégias de Influência Sino-Russas

A crescente sofisticação das operações de influência conduzidas por regimes autoritários, em particular pela Rússia e pela China, deve ser compreendida não como uma manifestação isolada de rivalidade geopolítica, mas como um fenómeno estruturalmente enraizado na ecologia de riscos globais do século XXI. A convergência tática, institucional e tecnológica entre Moscovo e Pequim não só reflete uma lógica de adaptação mútua, mas também atua como vetor amplificador de uma constelação de riscos interdependentes, que o *Global Risks Report 2024* do Fórum Económico Mundial identifica como centrais para a próxima década (*World Economic Forum*, 2024). O relatório posiciona a desinformação alimentada por inteligência artificial (IA) generativa como o risco mais grave no horizonte de dois anos, precisamente pelo seu poder de corroer os alicerces cognitivos das sociedades: a confiança, a coesão e a factualidade. Esta erosão epistémica é instrumentalizada de forma sistemática por regimes autoritários, cujas operações de influência recorrem a um arsenal de técnicas de saturação informacional, simulação de autenticidade e manipulação emocional, concebidas para perturbar a esfera pública e enfraquecer o consenso democrático (Pomerantsev, 2014; Goldstein, *et al*., 2023; Sobchuk, 2025; Darcy, *et al*., 2025).

A aliança tácita sino-russa tem-se revelado particularmente eficaz neste domínio. O citado caso *Spamouflage*, associado a redes coordenadas de contas falsas operadas a partir da China, evidencia não apenas uma replicação das práticas russas de manipulação reflexiva, mas também a integração de recursos técnicos avançados, como algoritmos de amplificação e conteúdo sintético, num modelo adaptativo e descentralizado de guerra informacional (*Graphika*, 2025). A "russificação" das operações externas chinesas traduz-se

numa mudança paradigmática no *modus operandi* de Pequim: passou de uma abordagem predominantemente defensiva e diplomática para uma estratégia ofensiva de disrupção informacional, inspirada no manual híbrido russo (Polyakova & Meserole, 2019). Esta convergência é reforçada por acordos institucionais e infraestruturas partilhadas, nomeadamente através de empresas como a *Huawei* e outras, cuja penetração global facilita tanto a vigilância estatal como a criação de ecossistemas digitais favoráveis à censura e à manipulação (Feldstein, 2019; Conselho da União Europeia; 2022). A colaboração bilateral entre meios de comunicação estatais e a realização regular de fóruns sino-russos no domínio da informação criam um espaço de interoperabilidade narrativa, onde se constroem e sincronizam discursos antiocidentais, revisionistas e conspiracionistas (Brady, 2017; Walker & Ludwig, 2017).

Importa ter em atenção que diversos documentos estratégicos, de alto nível, classificaram a China como o principal competidor e/ou adversário dos EUA com a intenção e, cada vez mais, a capacidade de remodelar a ordem internacional. Durante as presidências de John Biden e Trump, a administração norte-americana, através do *National Security Strategy* (2022), *National Defense Strategy* (2022), *Indo-Pacific Strategy of the United State*s (2022) e, mais recentemente, o *Annual Threat Assessment* (2024), identificou Pequim como a ameaça geopolítica mais abrangente e sistémica a longo prazo. A competição incidiria sobre áreas críticas como tecnologia, economia e influência global, numa lógica de evitar um conflito militar direto. As competências chinesas ao nível das atividades de espionagem, guerra cibernética e desinformação foram igualmente destacadas. Por seu turno, a Rússia foi referida como uma ameaça iminente e um ator disruptivo para a segurança regional europeia, focado na coação militar e em táticas de desestabilização, embora com capacidade limitada para competir à escala global. As análises sugerem ainda que

a China detém uma posição dominante, enquanto a Rússia está mais isolada e dependente, especialmente após a guerra na Ucrânia.

Mais preocupante é a forma compreensiva como estas operações sino-russas se articulam, oportunisticamente, com riscos ambientais e tecnológicos numa lógica de retroalimentação negativa. O *Global Risks Report 2024* enfatiza que os riscos não emergem de forma isolada, mas antes como complexos sistémicos interligados, em que a aceleração tecnológica, as alterações climáticas, as transformações demográficas e a fragmentação geopolítica se reforçam mutuamente (*World Economic Forum*, 2024). Neste quadro, a desinformação sobre alterações climáticas, muitas vezes promovida por atores ligados a regimes autoritários, tem um impacto direto na erosão do apoio público a políticas de mitigação e adaptação. A normalização da dúvida climática, potenciada por campanhas digitais coordenadas, mina os fundamentos da ação ambiental global, contribuindo para a inação institucional num momento crítico para o planeta (*World Economic Forum*, 2024 e 2025). Ao fomentar confusão, cinismo e paralisia política, as operações de influência sino-russas operam como verdadeiros multiplicadores de risco num ecossistema global já vulnerável. As campanhas conduzidas por Moscovo e Pequim não têm como objetivo apenas a imposição de uma narrativa alternativa, mas antes a fragmentação deliberada do real, o colapso da capacidade coletiva de distinguir entre a verdade e a falsidade, entre a análise racional e a reação emocional. Trata-se de um método operativo fundado na dissonância cognitiva e na disrupção sistemática, em perfeita consonância com o cenário de risco identificado: a erosão da verdade como ameaça à governança democrática, à resiliência ambiental e à segurança digital (Gouliev, 2025; Darcy, *et al*., 2025).

Tabela 1 - Análise SWOT da convergência sino-russa

SWOT	Rússia	China
Forças	▪ Experiência consolidada em operações de desinformação híbrida desde 2014 (Crimeia, Síria), em que a coordenação entre meios convencionais, redes sociais e grupos de hackers foi orquestrada ao nível estratégico. ▪ Utilização extensa de *firehose of falsehood* para saturar o espaço informativo com narrativas contraditórias, dificultando a refutação eficaz.	▪ Elevados recursos técnicos e financeiros canalizados para o desenvolvimento de IA e automação de campanhas, apoiados por uma sinergia Estado-empresas tecnológicas-exército. ▪ Narrativa de "capacidade civilizacional" e *soft power* económico, especialmente em África e América Latina, que viabiliza alianças políticas e culturais sustentadas.
Fraquezas	▪ Dependência de grupos de APT (APT28, APT29) hoje sob intenso escrutínio internacional, o que limita a sua margem de manobra sem captar contramedidas rápidas. ▪ Estilo de ação por vezes demasiado agressivo e óbvio, que catalisa contra-ataques legais, diplomáticos e de *fact-checking* coordenados (*EUvsDisinfo*, NATO *StratCom*).	▪ Barreiras linguísticas e culturais que enfraquecem a penetração direta em audiências ocidentais, obrigando a recorrer a intermediários locais. ▪ Rede de influência dispersa em múltiplos atores corporativos, dificultando uma coordenação centralizada e rápida resposta estratégica.
Oportunidades	▪ Explorar vulnerabilidades em democracias ocidentais marcadas por crises institucionais e económicas pós-pandemia, maximizando o impacto de narrativas de instabilidade. ▪ Adoção crescente de *deepfakes* para corroer a confiança pública em processos eleitorais futuros.	▪ Capitalizar em parcerias estratégicas com países do Sul Global (BRICS, África) para reforçar apoio político em fóruns multilaterais (ONU, G20). ▪ Intensificar o uso de IA generativa em *soft power* cultural (vídeos, memes, análises preditivas) para ampliar a capilaridade das mensagens sem grandes custos marginais.
Ameaças	▪ Fortalecimento de mecanismos de cooperação transatlântica de *fact-checking* e	▪ Crescente escrutínio global sobre violações de direitos humanos e censura,

	cibersegurança (*EUvsDisinfo*, NATO *StratCom*), reduzindo eficácia das operações híbridas. ▪ Sanções económicas e litigância internacional contra intermediários digitais, enquadrando legalmente muitos vetores de influência como atividades ilícitas.	que mina a credibilidade das narrativas oficiais. ▪ Possível rutura com parceiros ocidentais em caso de uso extremo de vigilância e tecnologia de controlo social, gerando desconfiança mesmo em países tradicionalmente alinhados.

***Fonte**: Elaboração própria, inspirada na investigação de Paul & Matthews, 2016; Kramer & Speranza, 2017; Brown, Chimits, & Sebastian, 2023; Gräf & Schmalz, 2023; Schuman, Fulton, & Gering, 2023;* Trellix Advanced Research Center, *2025; Boullenois, Kratz, & Rosen, 2025.*

5. IA e Guerra Cognitiva: Desafios à Confiança Pública e à Transparência

A emergência da IA transformou radicalmente o campo da desinformação, colocando a guerra cognitiva no cerne dos riscos globais modernos. Estudo recentes demonstram como atores russos ligados ao Estado cleptocrático estão a reconfigurar a guerra informacional através do uso de IA generativa, não apenas como ferramenta de amplificação automática, mas como elemento central de construção e moldagem das narrativas estratégicas, entroncando práticas que abrangem desde *deepfakes* a manipulação de grandes modelos linguísticos (Wallner, Copeland, & Giustozzi, 2025).

Paralelamente, a guerra cognitiva não deve ser encarada como uma simples campanha de desinformação, mas como um esforço sistemático para moldar perceções e decisões adversárias sem recurso à força física direta (Backes & Swab, 2019; Gouliev, 2025). Este tipo de guerra opera num *continuum* simbólico, político e psicológico, usando meios digitais, informacionais, económicos, diplomáticos e militares para alterar a realidade cognitiva dos alvos (Gräf & Schmalz, 2023; Solomon, 2025). Estas abordagens integram-se no quadro das ameaças híbridas associadas à cimeira da OTAN, tendo em conta as avaliações sobre os riscos que rodeiam os

encontros dos líderes aliados: desde ataques cibernéticos a operações informacionais, orquestradas com o objetivo de prejudicar a confiança na coesão da Aliança e amplificados por narrativas fabricadas ou filtradas por IA generativa (*Insikt Group*, 2025). Neste contexto, sobressai um paradigma híbrido onde a IA é usada para contaminar fontes informativas – um processo conhecido como *LLM grooming* – no qual atores diversos, como a rede estatal russa *Pravda*, inundam o envolvente cibernético com conteúdos falsos destinados a influenciar diretamente as respostas dos sistemas de geração de texto e imagem (Barbosa, 2016; Tril, 2025; Verhelst, 2025). Os vieses percetivos, heurísticas e processos interpessoais podem ser explorados por mensagens sofisticadas, uma vez que a manipulação não precisa ser manifesta ou evidente. A introdução de mapas de credibilidade parcial, sombras de verdade e indeterminação semântica bastam para desorganizar a lógica individual e coletiva (Feldstein, 2019; NATO | OTAN, 2024; Darcy, *et al*., 2025).

Recordamos que, em janeiro de 2025, o Parlamento Europeu condenou formalmente a guerra de agressão levada a cabo pela Rússia contra a Ucrânia, repudiando a estratégia de desinformação utilizada para a sua legitimação e apelando ao reforço das medidas de combate aos canais infodémicos (Fernandes, 2025). A este respeito, a Resolução P10_TA (2025)0006 representa um marco relevantíssimo, na medida em que reconhece que a falsificação da história é parte integrante de uma estratégia de guerra híbrida e informação manipulada. Complementarmente, o Parlamento Europeu propõe sanções específicas contra os meios de comunicação russos que difundem desinformação; encoraja o apoio aos média russos independentes no exílio, reforçando a diversidade informativa em língua russa, e exige a devida aplicação de regulamentações europeias, como o *Digital Services Act*, para maximizar a moderação e mitigar a propagação de mentiras nas plataformas digitais

Concretizando o modelo de influência autoritária sino-russo, certificamos que o mesmo está estruturado em três eixos inter-relacionados. Primeiramente, assenta na automatização e amplificação via IA. Neste domínio, os regimes autoritários profissionais combinam mensagens parciais e *deepfakes* com redes automatizadas, criando um ecossistema de saturação informacional que escraviza tanto o humano quanto o modelo artificial a respostas enviesadas, instáveis e contraditórias (Goldstein, *et al*., 2023; Wallner, Copeland, & Giustozzi, 2025). O segundo vetor é a manipulação cognitiva transversal, através do qual a estratégia de guerra (russa) da informação e da perceção sustenta-se na ambiguidade estratégica, utilizando utilizar verdades parciais e falsificações para distorcer o raciocínio e enfraquecer a vontade política dos adversários, sobretudo em contextos de cimeiras internacionais onde discursos e decisões são públicos e altamente visíveis (Solomon, 2025). Por fim, temos o eixo da exposição das vulnerabilidades democráticas, tal como se verificou com a última cimeira da OTAN, conhecida como a Cimeira da Haia de 2025. Neste contexto, múltiplos atores estatais ativistas, recorrendo à espionagem digital e a operações de influência[9] dedicadas a criar cismas internos entre os aliados, espalharam narrativas de desunião, legitimidade forjada e disfunção institucional, intensificadas por conteúdo fabricado por IA e vazamentos operacionais (Conselho da União Europeia; 2022; *Insikt Group*, 2025).

Em síntese, certificamos que as operações de influência modernas usam a IA não apenas para expandir o alcance, como

[9] A presidente do Serviço de Contraespionagem Militar da Alemanha (MAD), Martina Rosenberg, alertou para um aumento acentuado das atividades de espionagem e operações híbridas na Alemanha, sobretudo por parte da Rússia. Segundo Rosenberg, estas ações tornaram-se mais amplas e agressivas, incluindo ciberataques, campanhas de desinformação e tentativas de sabotagem, com alvos ligados ao apoio alemão à Ucrânia. As autoridades alemãs registaram o dobro de casos suspeitos em 2025, sublinhando a crescente ameaça à segurança nacional (Verhelst, 2025).

também para reconfigurar os princípios epistemológicos dos diferentes públicos. Por outro lado, a guerra cognitiva tornou-se uma linha de frente invisível: as decisões políticas são calibradas não segundo factos, mas de acordo com narrativas enviesadas que subvertem a perceção do real (Backes & Swab, 2019). Finalmente, as cimeiras internacionais constituem laboratórios operacionais cruciais, onde se testam e refinam tanto a desinformação com IA integrada quanto os modos de enfraquecimento institucional. Este paradigma exige respostas estratégicas interdisciplinares e interoperativas. A monitorização em tempo real, a inteligência preditiva baseada em IA, a educação mediática sofisticada e a estreita coordenação entre aliados são tidas como fundamentais para proteger infraestruturas físicas e, sobretudo, a própria lógica da verdade compartida (Feldstein, 2019; Wasinger, *et al*., 2024).

Tabela 2 - Mapa de Riscos e Respostas

Risco Global Identificado	**Conexão com Operações Sino-Russas**	**Ator Democrático**	**Recomendações de Resiliência**
Desinformação em processos eleitorais	Campanhas de *bots* e *trolls* financiadas e coordenadas a partir da Rússia e da China para semear dúvidas sobre instituições	Comissões eleitorais independentes; observatórios de *fact-checking*	Fortalecer legislação sobre transparência de anúncios políticos *online*. Criar parcerias público-privadas de monitorização em tempo real. Promover literacia mediática nas escolas.
Ciberataques a infraestruturas críticas	Utilização de grupos de hackers pró-estado (APT28, APT41)	Agências nacionais de cibersegurança;	Implementar exercícios regulares de *red*

	para testar vulnerabilidades e desestabilizar sistemas energéticos e de comunicações	NATO*Cyber Defence Centr e*	*teaming* em estruturas críticas. Partilhar indicadores de comprometimento (IoCs) entre países aliados. Financiar pesquisa em ciber-resiliência industrial.
Erosão da confiança nas instituições democráticas	Campanhas de *Spamouflage* que associam governos ocidentais a narrativas de corrupção e violação de direitos	Parlamentos nacionais e instituições judiciais	Transparência proativa de dados governamentais. Programas de participação cívica com audiências fora dos grandes centros. Observatórios académicos independentes de governança pública.
Polarização e fragmentação social	Financiamento de conteúdos em redes sociais que exploram clivagens étnicas, religiosas e ideológicas	ONG de direitos humanos; plataformas digitais reguladas	Regulamentação de algoritmos de recomendação para evitar câmaras de ressonância. Campanhas de diálogo intercomunitário mediadas por facilitadores treinados. Mecanismos de denúncia

			simplificados nas plataformas.
Crises geopolíticas regionais e escalada militar	Apoio informacional a movimentos separatistas e ministração de *soft power* para legitimar intervenções militares	Ministérios dos Negócios Estrangeiros; Missões de paz da ONU	Mecanismos multilaterais de *early warning* (EDI – Estado, Diáspora, Intelectuais). Iniciativas de diplomacia pública conjunta UE- OTAN. Programas de mediação cultural e intercâmbios académicos.

***Fonte**: Elaboração própria, inspirada na investigação de Snegovaya, 2015;* European Union External Action*, 2023; NATO | OTAN, 2024; Wasinger,* et al.*, 2024;* World Economic Forum*, 2024.*

Conclusão

O presente artigo procurou explorar, de forma integrada, a emergência da guerra informacional como eixo estratégico central das rivalidades geopolíticas contemporâneas, com especial enfoque nas práticas coordenadas entre a Federação Russa e a República Popular da China. A dinâmica em evolução insinua uma interação complexa em que a China investe estrategicamente em recursos mínimos para obter influência substancial sobre a Rússia, a Ásia Central e a Europa, descortinando um panorama geopolítico implexo e multipolar. Através da articulação dos conceitos de guerra – híbrida, cognitiva e de influência –, evidenciou-se a crescente sofisticação dos métodos utilizados por regimes autocráticos para perturbar o ecossistema informacional global, manipular perceções coletivas e enfraquecer os pilares da governança democrática.

A análise demonstrou como estas operações evoluíram de instrumentos pontuais de propaganda para sistemas complexos de disrupção cognitiva, onde se entrelaçam estratégias digitais, infraestruturas tecnológicas partilhadas e alianças institucionais duradouras (Bayer, *et al*., 2021). A icónica campanha *Spamouflage*, a interoperabilidade mediática sino-russa e o uso crescente da IA generativa revelam a enorme adaptabilidade destas operações e a sua ambição de modelar o próprio "regime de verdade" global. Neste quadro, a instrumentalização da IA no domínio da informação digital evidencia uma viragem paradigmática: a *infowar* deixou de visar apenas os conteúdos para passar a operar sobre os próprios mecanismos de perceção, credibilidade, cognição e decisão (Arquilla & Ronfeldt, 1993). A manipulação já não se limita à mentira explícita, mas recorre à ambiguidade, à sobrecarga semântica, à repetição e à fragmentação epistémica como armas principais. A verdade, enquanto recurso partilhado e estruturante da ação política, torna-se o principal alvo a corromper (Conselho da União Europeia, 2022; Dugin, 2025).

As operações sino-russas representam uma manifestação operacional dos riscos globais interconectados. Ao instrumentalizar a desinformação alimentada pela IA, estas técnicas não só promovem polarização social, como sabotam as capacidades adaptativas perante o colapso ambiental e o enfraquecimento das estruturas de cooperação global. Num momento onde os riscos tecnológicos, ambientais e societais se reforçam mutuamente, tais operações subvertem os fundamentos da verdade, da confiança e da resiliência internacional. Conforme identificado no *Global Risks Report 2024*, a desinformação e a fragmentação cognitiva não são riscos isolados, mas catalisadores de crises mais vastas que vão desde as alterações climáticas à disfunção democrática, da insegurança digital à erosão da coesão social. Assim, as operações sino-russas não são apenas sintoma de competição geopolítica, mas agentes ativos da desestruturação

global. Mais do que uma crise circunstancial, a confrontação entre o Eixo dos Autoritários – com a Rússia e a China em destaque – e a Aliança Ocidental em torno da Ucrânia constitui um sintoma de uma divergência profunda entre as visões que cada lado tem do mundo. Tudo indica que este choque perdurará enquanto o Ocidente continuar a apoiar a independência e a soberania plena dos Estados da "linha da frente", ou seja, daqueles territórios que a Rússia encara como parte do seu espaço de influência legítimo (Kuczyńska-Zonik, 2016; Cardoso, 2022). Acresce, portanto, a essencialidade de reconhecer que os valores e interesses vitais do Ocidente não são conciliáveis com os do bloco autocrático, especialmente com os da Rússia, de modo a ajustar a gestão da relação bilateral, senão multilateral, em função da erosão da incompatibilidade. Recordamos as palavras de Winston Churchill, que afirmou que "(…) desde que o mundo livre se mantenha unido e forte (…), a Rússia descobrirá que a paz e a abundância têm mais para oferecer do que uma guerra de extermínio. Alargar o pensamento é um processo que adquire ímpeto quando se procura um mundo em que todos podem desfrutar de oportunidades. Pode bem acontecer que, se a sagacidade e a paciência forem praticadas, esse ambiente de oportunidades para todos conquiste as mentes e restrinja as paixões da Humanidade" (Churchill, 2011, pp. 202–203). Enquanto a proposta de Churchill não se materializar, a resposta a este confronto existencial, mais do que soluções técnicas ou estritamente regulamentares, perpassa por uma reconceptualização das políticas de segurança, educação e diplomacia à luz da nova condição cognitiva do conflito. Importa, pois, aprimorar uma arquitetura de resiliência epistémica, reforçar a literacia mediática em todos os níveis da sociedade e consolidar alianças democráticas, não só em termos militares, securitários ou económicos, mas também no plano informacional e simbólico. Só assim será possível proteger não apenas territórios e infraestruturas,

mas o próprio espaço partilhado da verdade, a condição *sine qua non* para a liberdade, cooperação e sobrevivência numa ordem mundial em transformação (Comissão Europeia, 2025).

Aqui chegados, recomenda-se a adoção de um conjunto articulado de medidas integradas que envolvam os sectores público, académico e educativo. Em termos de políticas públicas, impõe-se a urgente criação de um quadro regulatório robusto para o uso de IA generativa em campanhas políticas, que compelira os responsáveis pelo financiamento e pela difusão de anúncios eleitorais a identificar e filtrar conteúdos gerados artificialmente, sob pena de sanções administrativas e criminais. Simultaneamente, deve-se exigir a transparência absoluta nos financiamentos digitais, obrigando à publicação pública, em plataformas oficiais, dos montantes investidos, das suas origens e dos respetivos destinos, de modo a inibir operações opacas de influência. Por fim, a avaliação de impacto de novas funcionalidades em redes sociais torna-se indispensável. A obrigatoriedade destas apreciações prévias permitiria antever e mitigar potenciais utilizações maliciosas dos algoritmos de recomendação, protegendo o espaço público de desvios manipulativos (Pamment, 2020; Fernandes 2025a).

No plano académico, a constituição de um observatório multidisciplinar e colaborativo de desinformação assume papel central, congregando universidades, *think tanks* e centros de investigação numa plataforma internacional destinada à recolha sistemática, análise rigorosa e divulgação transparente de dados sobre campanhas de desinformação, com *dashboards* acessíveis que sinalizem tendências emergentes e pontos quentes de atividade maliciosa. A par desta iniciativa, urge fomentar redes de investigação multidisciplinares que articulem as perspetivas das Relações Internacionais, da Ciência dos Dados e da Psicologia Social, de modo a

decifrar, em profundidade, a amplitude e os efeitos das narrativas manipulativas em distintos contextos culturais e cognitivos. Acresce a necessidade de desenvolver revisões sistemáticas dinâmicas, permanentemente atualizadas com novas evidências sobre táticas de influência, garantindo aos decisores políticos e aos profissionais de comunicação acesso contínuo às descobertas mais recentes e empiricamente fundamentadas.

No domínio da literacia mediática, é premente inserir, no currículo de escolas e universidades, módulos práticos de análise crítica de fontes, verificação de factos e deteção de deepfakes, capacitando os estudantes para um consumo informativo crítico, consciente e resistente a manipulações. Simultaneamente, devem ser concebidos workshops especializados para jornalistas e comunicadores, que incluam simulações realistas de ataques cibernéticos, conduzidas por uma equipe especializada com o objetivo de testar a eficácia das defesas de segurança (vulgo, exercícios de red teaming) e a análise de casos reais de operações coordenadas de desinformação, fortalecendo as competências de deteção precoce e resposta a ataques cognitivos. Por último, campanhas de sensibilização pública, desenvolvidas em parceria com organizações não governamentais e plataformas digitais, poderão promover o uso generalizado de ferramentas de verificação e cultivar hábitos críticos de consumo jornalístico na sociedade em geral. Sublinhamos que, neste particular, a UE, através da EUROPOL e de outros organismos e agências, tem incrementado múltiplas estratégias de *fact-checking* para mitigar os efeitos das operações FIMI conexas à aliança sino-russa, investindo na desarticulação de redes de desinformação, no reforço da literacia mediática e na produção de inteligência policial (Fernandes, 2025).

A convergência destas políticas, estratégias, iniciativas e práticas reforçará, de modo decisivo, a capacidade de resposta às

ameaças híbridas e contribuirão para a construção de uma esfera pública mais informada, resiliente e capaz de sustentar os valores democráticos. Tenhamos consciência que, perante a incompatibilidade estrutural entre os interesses estratégicos sino-russos e os valores fundamentais da Aliança Ocidental, impõe-se uma escolha derradeira à UE: ou investe, de forma consistente e prolongada, numa política de dissuasão eficaz, assente em capacidades que o bloco autocrático reconheça como credíveis; ou assume o abandono dos Estados da *Rimland* europeia e, com eles, da defesa dos princípios que sustentam a ordem liberal ocidental (Kaplan, 2022). Reconhecer esta dicotomia e reorientar, em conformidade e com assertividade, as políticas de defesa, segurança e investimento reveste, neste momento, condição essencial para salvaguardar a paz e a estabilidade no espaço europeu (Dirsus, 2025). Só assim seremos capazes de conter a ofensiva autocrática, valorizar a diplomacia estabilizadora e defender a UE do "*rocket*" de influxo despótico, restituindo-o ao remetente euroasiático com uma mensagem clara: *Cives Europaei sumus*[10].

Omnes Omnibus

[10] Expressão latina que significa "somos cidadãos europeus" (tradução livre).

Referências

Agência Lusa. (18 de julho de 2025a). Paris alvo de "campanha de desinformação sem precedentes". Observador. Obtido em 20 de julho de 2025, de https://observador.pt/2025/07/18/franca-esta-a-ser-alvo-de-campanha-de-desinformacao-sem-precendentes/

Agência Lusa. (22 de julho de 2025b). YouTube remove quase 11 mil canais ligados à propaganda da China e da Rússia. Público. Obtido em 23 de julho de 2025, de Público. https://www.publico.pt/2025/07/22/enter/noticia/youtube-remove-quase-11-mil-canais-ligados-propaganda-china-russia-2141279

Aktas, A. (11 de julho de 2025). Kremlin slams Europe's 'refusal to hear' signals on foreign troops in Ukraine. Obtido em 30 de julho de 2025, de www.aa.com.tr: https://www.aa.com.tr/en/russia-ukraine-war/kremlin-slams-europe-s-refusal-to-hear-signals-on-foreign-troops-in-ukraine/3628196

Alexandre, R. (05 de março de 2025). Ucrânia vs. EUA: alguns pormenores sobre o acordo dos minerais. SIC Notícias. Obtido em 02 de abril de 2025, de https://sicnoticias.pt/especiais/guerra-russia-ucrania/2025-03-05-video-ucrania-vs.-eua-alguns-pormenores-sobre-o-acordo-dos-minerais-fcb7274c

Applebaum, A. (2024). Autocracia, Inc. - Os ditadores que querem governar o mundo (1.ª ed.). (J. Gafeira, Trad.) Lisboa: Bertrand Editora.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! Comparative Strategy, 12(2), p. 28.

Backes, O., & Swab, A. (2019). Cognitive Warfare. The Russian Threat to Election Integrity in the Baltic States. Cambridge: Belfer Center for Science and International Affairs.

Barbosa, M. L. (July/December de 2016). As ameaças ao ciberespaço e a estratégia de cibersegurança na UE e em Portugal. RDeS – Revista de Direito e Segurança(8), pp. 161-187. Obtido em 15 de July de 2025, de https://www.jorgebacelargouveia.com/wp-content/uploads/2020/08/Revista-RDeS-n%C2%BA-8-on-line.pdf#page=163

Barnes, J., Kelly, K., & Mendick, R. (18 de julho de 2025). Unmasked: The Russian spies who targeted Britain on Putin's orders. The Telegraph. Obtido em 20 de julho de 2025, de https://www.telegraph.co.uk/world-news/2025/07/18/russian-spies-targeted-britain-unmasked-putin/

Bayer, J., Holznagel, B., Lubianiec, K., Pintea, A., Schmitt, J. B., Szakács, J., & Uszkiewicz, E. (2021). Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States - 2021 update. Think Tank - European Parliament. Obtido em 23 de julho de 2025, de http://www.europarl.europa.eu/RegData/etudes/STUD/2021/653633/EXPO_STU(2021)653633_EN.pdf

Bochantin, L. (25 de abril de 2024). How Russian Telegram Framed Taiwan's Elections and Sovereignty. Doublethink Lab. Obtido em 22 de julho de 2024, de https://medium.com/doublethinklab/how-russian-telegram-framed-taiwans-elections-and-sovereignty-894ef08694cc

Bond, S. (29 de 08 de 2023). Meta says Chinese, Russian influence operations are among the biggest it's taken down. npr. Obtido em 17 de julho de 2025, de https://www.npr.org/2023/08/29/1196117574/meta-says-chinese-russian-influence-operations-are-among-the-biggest-its-taken-d

Boullenois, C., Kratz, A., & Rosen, D. H. (2025). Far From Normal: An Augmented Assessment of China's State Support. Rhodium Group. Obtido em 23 de julho de 2025, de https://rhg.com/research/far-from-normal-an-augmented-assessment-of-chinas-state-support/

Brady, A.-M. (18 de setembro de 2017). Magic Weapons: China's political influence activities under Xi Jinping. Wilson Center. Obtido de https://www.wilsoncenter.org/article/magic-weapons-chinas-political-influence-activities-under-xi-jinping

Brands, H., & Gaddis, J. L. (2021). The new cold war. Foreign Affairs, 6(100), pp. 10-21.

Bremmer, I. (2018). Us vs. them: The failure of globalism. Penguin.

Brown, A., Chimits, F., & Sebastian, G. (2023). Accelerator state: How China fosters "little giant" companies. Mercator Institute for China Studies (MERICS). Obtido em 25 de julho de 2025, de https://merics.org/en/report/accelerator-state-how-china-fosters-little-giant-companies

Cardoso, R. (2022). Ucrânia - 35 pontos fundamentais para entender a invasão russa (3.ª ed.). (F. Camacho, Ed.) Oficina do Livro.

Churchill, W. (2011). Memórias da Segunda Guerra Mundial. Edição resumida com um epílogo referente aos anos 1945 a 1957 (Vol. IV). (M. Cabral, Trad.) Texto Editores.

Cláudio, V. (2015). A Rússia e o neo-Eurasianismo. EuroDefense Portugal. Lisboa: EuroDefense Portugal. Obtido em 02 de abril de 2025, de https://eurodefense.pt/a-russia-e-o-neo-eurasianismo/

Comissão Europeia. (01 de abril de 2025). ProtectEU: Uma Estratégia Europeia de Segurança Interna. Estrasburgo: Comissão Europeia. Obtido em 01 de abril de 2025, de https://commission.europa.eu

Conselho da União Europeia. (2022). Conclusões do Conselho sobre manipulação de informações e ingerências por parte de agentes estrangeiros. Bruxelas: Secretariado-Geral do Conselho da União Europeia. Obtido em 15 de maio de 2025, de https://data.consilium.europa.eu/doc/document/ST-11429-2022-INIT/pt/pdf

Costa, F. S. (28 de julho de 2025). Trump 15 – Europa 0. (F. S. Costa, Ed.) Obtido em 28 de julho de 2025, de Duas ou três coisas (blogspot): https://duas-ou-tres.blogspot.com/2025/07/trump-15-europa-0.html

Creemers, R. (2018). Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century. Em R. Creemers, Chinese Authoritarianism in the Information Age (p. 16). Routledge.

Cull, N. (2009). Public diplomacy: Lessons from the past (Vol. 12). Los Angeles: Figueroa Press.

Darcy, G., Mercier, H., Mari, A., Casati, R., Origgi, G., & Yahia, L. (2025). Lutter contre la désinformation : Penser autrement l'action publique à l'aune des sciences cognitives | Rapport sur la Désinformation. Institut Jean Nicod; Département d'Études Cognitives; École Normale Supérieure - PSL. doi:https://doi.org/10.31219/osf.io/fu9cz_v1

Dirsus, M. (2025). Como caem os tiranos e como sobrevivem as nações (1.ª ed.). (C. A. Nogueira, Ed., & C. P. Martins, Trad.) Desassossego.

Dugin, A. (1997). Foundations of geopolitics. Moskva: Arktogeja-centr.

Dugin, A. (2025). The Trump Revolution: A New Order of Great Powers. Arktos Media Ltd.

Dukach, Y., Adam, I., & Furbish, M. (2025). Digital occupation: Pro-Russian bot networks target Ukraine's occupied territories on Telegram. Atlantic Council. Obtido em 21 de julho de 2025, de https://www.atlanticcouncil.org/in-depth-research-reports/report/report-russian-bot-networks-occupied-ukraine/

Duranty, W. (1944). USSR: The Story of Soviet Russia. New York: J.B. Lippincott.

European Court of Auditors. (2020). EU Action Plan Against Disinformation. European Union - European Court of Auditors (ECA). Obtido em 23 de julho de 2025, de https://www.eca.europa.eu/lists/ecadocuments/ap20_04/ap_disinformation_en.pdf

European Union External Action. (2023). EEAS Stratcom's responses to foreign information manipulation and interference (FIMI) in 2023 - Highlights. Strategic Communication and Foresight (SG.STRAT). Obtido em 23 de julho de 2025, de https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS%20Stratcom%20Annual%20Report%202023.pdf

Feldstein, S. (setembro de 2019). The global expansion of AI surveillance. Carnegie Endowment for International Peace, 17(9).

Fernandes, R. N. (2024a). 2024: A soma de todos os riscos geopolíticos. (P. Machado, Ed.) Politeia - Revista Portuguesa de Ciências Policiais(XXI). Obtido de https://comum.rcaap.pt/handle/10400.26/58015

Fernandes, R. N. (2024b). The Police Diplomat Network as a response to Modern Challenges: A Portuguese Perspective. Security Spectrum: Journal of Advanced Security Research(23), pp. 48-74. doi:https://doi.org/10.15158/eear-6856

Fernandes, R. N. (2024c). The New Thinking of Police Diplomacy in the Context of International Coopetition. Internal Security, 16(2), pp. 133-155. doi:https://doi.org/10.5604/01.3001.0055.0887

Fernandes, R. N. (2025). Outlets de Desinformação na Nova Geopolítica Digital (1.ª ed.). (R. N. Fernandes, Ed.) Lisboa: Centro de Investigação (ICPOL) do Instituto Superior de Ciências Policiais e segurança Interna (ISCPSI).

Ferreira, M. F., & Terrenas, J. (2016). Good-bye, Lenin! Hello, Putin! O discurso geoidentitário na política externa da nova Rússia. Revista Brasileira de Ciência Política(20), pp. 43-78. doi:https://doi.org/10.1590/0103-335220162002

Freedman, L. (2015). Strategy: A history. Oxford University Press.

Galeotti, M. (2022). Putin's wars: from Chechnya to Ukraine. Bloomsbury Publishing.

Giles, K. (março de 2016). Russia's 'new'tools for confronting the West: Continuity and innovation in Moscow's exercise of power. Chatham House - The Royal Institute of International Affairs, p. 73. Obtido em 22 de julho de 2025, de https://d1wqtxts1xzle7.cloudfront.net/43933484/2016-03-21-russias-new-tools-giles-libre.pdf?1458520166=&response-content-disposition=inline%3B+filename%3DRussia_s_New_Tools_for_Confronting_the_W.pdf&Expires=1753198023&Signature=OCPe8ylsS6BiXsDX8I6~lLHPtI0

Goldstein, J. A., Sastry, G., Musser, M., DiResta, R., Gentzel, M., & Sedova, K. (janeiro de 2023). Generative language models and automated influence operations: Emerging threats and potential mitigations. Stanford Internet Observatory; OpenAI; Center for Security and Emerging Technology (CSET) da Georgetown University. Plataforma arXiv. Obtido de https://d1wqtxts1xzle7.cloudfront.net/100983602/2301.04246-libre.pdf?1681244354=&response-content-disposition=inline%3B+filename%3DGenerative_Language_Models_and_Automated.pdf&Expires=1753201358&Signature=OwEP7~9bK8IO5YAXWRfybYCQgkckTNWDL9h8AuRw68F7d1aeRE

Gouliev, Z. (2025). Disinformation-as-a-Service: Rise of the "Influence Operators". CEPOL Research & Science Conference 2024/2025. Óstia, Itália: CEPOL.

Gräf, H., & Schmalz, S. (2023). Avoiding the China shock: How Chinese state-backed internationalization drives changes in European economic governance. Competition & Change. doi:10.1177/10245294231207990

Graphika. (2025). Chinese State Influence - Selected Insights from Graphikas's ATLAS Intelligence Reporting on Chinese State Influence Actors and Adjacent Communities. Graphika . Obtido em 25 de julho de 2025, de https://public-assets.graphika.com/atlas-highlights-china.pdf

Hebdige, D. (2013). Subculture. Routledge.

Hill, F., & Gaddy, C. G. (2015). Mr. Putin REV: Operative in the Kremlin. Brookings Institution Press.

Hobsbawm, E. (1995). Era dos extremos: o breve século XX. Editora Companhia das Letras.

Hoffman, F. G. (2014). Hybrid warfare and challenges. Strategic studies, pp. 329-337.

Hvistendahl, M., & Kovalev, A. (30 de dezembro de 2022). Hacked Russian files reveal propaganda agreement with China - n 2021, government officials and media executives from Russia and China discussed the exchange of news and social content. The Intercept. Obtido em 23 de julho de 2025, de https://theintercept.com/2022/12/30/russia-china-news-media-agreement/

Insikt Group. (2025). Threats to the 2025 NATO Summit. Insikt Group®. Obtido em 23 de julho de 2025, de https://www.recordedfuture.com/research/threats-2025-nato-summit

Institute for Economics & Peace. (2025). Global Peace Index 2025: Identifying and measuring the factors that drive peace. Sydney: Institute for Economics & Peace (IEP). Obtido em 22 de julho de 2025, de https://www.economicsandpeace.org/wp-content/uploads/2025/06/GPI-2025-web.pdf

Institute for Strategic Dialogue. (01 de abril de 2024). Pro-CCP Spamouflage campaign experiments with new tactics targeting the US. ISD - Digital Dispaches. Obtido em 22 de julho de 2025, de https://www.isdglobal.org/digital_dispatches/pro-ccp-spamouflage-campaign-experiments-with-new-tactics-targeting-the-us/

Intrisec. (2025). From espionage to PsyOps: Tracking operations and bulletproof providers of UACs in 2025. Intrisec. Obtido em 22 de abril de 2024, de https://www.intrinsec.com/from-espionage-to-psyops-tracking-operations-and-bulletproof-providers-of-uac/?cn-reloaded=1

Kaplan, R. D. (2022). A vingança da Geografia. (F. e. Silva, Trad.) Lisboa: Clube do Autor.

Kissinger, H. (2014). Henry Kissinger: To settle the Ukraine crisis, start at the end. The Washington Post(5).

Kofman, M., Migacheva, K., Nichiporuk, B., Radin, A., & Oberholtzer, J. (2017). Lessons from Russia's operations in Crimea and Eastern Ukraine. Rand Corporation. Obtido em 13 de julho de 2025, de https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1498/RAND_RR1498.pdf

Kramer, F. D., & Speranza, L. M. (02 de junho de 2017). Meeting the Russian Hybrid Challenge: A Comprehensive Strategic Framework. Atlantic Council. Obtido em 28 de julho de 2025, de https://www.atlanticcouncil.org/blogs/natosource/meeting-the-russian-hybrid-challenge-a-comprehensive-strategic-framework-2/

Kruttke, C. (2024). Displacement and Disinformation: How Russia is Instrumentalizing Migration and Disinformation as a Foreign Policy Tool against the European Union. Enschede: University of Twente.

Kuczyńska-Zonik, A. (2016). Russian propaganda: methods of influence in the Baltic States. Rocznik Instytutu Europy Środkowo-Wschodniej, 2(14), pp. 43-59.

Lake, D. A., Martin, L. L., & Risse, T. (2021). Challenges to the Liberal Order: Reflections on International Organization. International Organization, 2(75), pp. 225–257. doi:10.1017/S0020818320000636

Meta. (2023). Threat report: April 2023 – Taking down the Spamouflage influence operation. Meta Platforms, Inc. Obtido em 17 de julho de 2025, de https://about.fb.com/news/2023/04/taking-down-spamouflage-influence-operation/

Moysan, E. (09 de julho de 2025). L'Europe en première ligne des ingérences informationnelles russes. Alternatives Economiques. Obtido em 21 de julho de 2025, de https://www.alternatives-economiques.fr/leurope-premiere-ligne-ingerences-informationnelles-russes/00115455

NATO | OTAN. (2024). Hybrid Threats and Hybrid Warfare Reference Curriculum (HTHWRC). Brussels: NATO | OTAN.

Nye, J. S. (2008). Public diplomacy and soft power. The annals of the American academy of political and social science, 1(616), pp. 94-109. doi:https://doi.org/10.1177/00027162073116

Nye, J. S. (2023). Soft power and great-power competition: Shifting sands in the balance of power between the United States and China. Springer Nature.

Olszański, T. A., Sarna, A., & Wierzbowska-Miazga, A. (19 de março de 2014). The consequences of the annexation of Crimea. Analyses. OSW | Centre For Eastern Studies. Obtido em 02 de abril de 2025, de https://www.osw.waw.pl/en/publikacje/analyses/2014-03-19/consequences-annexation-crimea

Pamment, J. (2020). The EU's role in fighting disinformation: taking back the initiative. Carnegie Endowment for International Peace. Obtido em 23 de julho de 2025, de https://carnegie-production-assets.s3.amazonaws.com/static/files/Pamment_-_Future_Threats.pdf

Patton, M. Q. (2002). Qualitative research and evaluation methods. California: Sage Publications, Inc. Obtido em 18 de julho de 2025, de https://aulasvirtuales.wordpress.com/wp-content/uploads/2014/02/qualitativeresearch-evaluation-methods-by-mich

Paul, C., & Matthews, M. (11 de julho de 2016). The Russian "Firehose of Falsehood" Propaganda Model - Why It Might Work and Options to Counter It. RAND Corporation - Perspective | Expert insights on a timely policy issue, p. 16. Obtido em 26 de julho de 2025, de https://www.rand.org/pubs/perspectives/PE198.html

Polyakova, A., & Meserole, C. (2019). Democracy & Disorder: Exporting digital authoritarianism: The Russian and Chinese models. Foreign Policy, pp. 1-22. Obtido em 24 de julho de 2025, de https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf

Pomerantsev, P. (2014). Nothing is true and everything is possible: The surreal heart of the new Russia. Public Affairs.

Pomerantsev, P. (2017). Nothing is true and everything is possible: Adventures in modern Russia. Faber & Faber.

Reagan, R. (2024). A Previsão do Colapso do Comunismo. Em M. Robalo (Ed.), 50 Grandes Discursos da História (J. Rosa, S. Carvalho, & L. Anjos, Trads., 2.ª ed., pp. 215-221). Lisboa: Edições Sílabo.

Reyes, R. (17 de julho de 2025). Russia must be ready to strike the West if it escalates the war in Ukraine, Kremlin says. . New York Post. Obtido em 29 de julho de 2025, de https://nypost.com/2025/07/17/world-news/russia-must-be-ready-to-strike-the-west-if-it-escalates-the-war-in-ukraine-kremlin-says/

Sahuquillo, M. R. (19 de dezembro de 2024). Zelenski admite ante la UE que sin Estados Unidos "es muy difícil mantener el apoyo a Ucrania". El País. Obtido em 13 de março de 2025, de https://elpais.com/internacional/2024-12-19/zelenski-admite-ante-la-ue-que-sin-estados-unidos-es-muy-dificil-mantener-el-apoyo-a-ucrania.html?utm_source=chatgpt.com

Sakwa, R. (2021). Russian Politics and Society (6.ª ed.). Routledge.

Salt, A., & Sobchuk, M. (agosto de 2021). Russian cyber-operations in ukraine and the implications for NATO. Canadian Global Affairs Institute. Obtido em 12 de junho de 2021, de https://d3n8a8pro7vhmx.cloudfront.net/cdfai/pages/4787/attachments/original/1629910505/Russian_Cyber-Operations_in_Ukraine_and_the_Implications_for_NATO.pdf?1629910505

Schuman, M., Fulton, J., & Gering, T. (21 de junho de 2023). How Beijing's newest global initiatives seek to remake the world order. Atlantic Council. Obtido em 29 de julho de 2025, de https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/how-beijings-newest-global-initiatives-seek-to-remake-the-world-order/

Shambaugh, D. (janeiro de 2007). China's propaganda system: Institutions, processes and efficacy. The China Journal(57), pp. 25-58. doi:https://doi.org/10.1086/tcj.57.20066240

Sheridan, D. (11 de julho de 2025). Britain 'must prepare for war with Russia in next five years'. The Telegraph. Obtido em 12 de julho de 2025, de https://www.telegraph.co.uk/news/2025/07/11/britain-must-prepare-for-war-with-russia-next-five-years/

Sheridan, M. (2025). O Imperador Vermelho: Xi Jinping e a Nova China (1.ª ed.). (M. R. Furtado, Trad.) Lisboa: Bertrand Editora.

Snegovaya, M. (setembro de 2015). Putin's information warfare in Ukraine. Soviet Origins of Russia's Hybrid Warfare'. (I. f. (ISW), Ed.) Russi Report I. Obtido em 22 de julho de 2025, de https://www.jstor.org/stable/pdf/resrep07921.1.pdf

Snyder, T. (6 de setembro de 2022). Ukraine holds the future: The war between democracy and nihilism. Foreign Affairs(101; 124). Obtido em 11 de julho de 2025, de https://www.foreignaffairs.com/ukraine/ukraine-war-democracy-nihilism-timothy-snyder

Sobchuk, M. (2025). To understand the nature of modern Chinese influence operations, study Russia first. Cyfluence Research Center. Obtido em 11 de julho de 2025, de https://download-files.wixmp.com/ugd/effca5_b320c368dd1e4fedb832f7bccebac76e.pdf?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJ1cm46YXBwOmU2NjYzMGU3MTRmMDQ5MGFhZWExZjE0OWIzYjY5ZTMyIiwic3ViIjoidXJuOmFwcDplNjY2MzBlNzE0ZjA0OTBhYWVhMWYxNDliM2I2OWUzMiI

Solomon, C. (2025). A Primer on Russian Cognitive Warfare. United States of America: Institute for the Study of War (ISW). Obtido em 22 de julho de 2025, de https://coilink.org/20.500.12592/3dqpprd

Thomas, T. (2004). Russia's reflexive control theory and the military. Journal of Slavic Military Studies, 2(17), pp. 237-256.

Todd, E. (2025). A Derrota do Ocidente. Principia Editora.

Trellix Advanced Research Center. (2025). The Cyberthreat Report - Insights Gleaned from a Global Network of Experts, Sensors, Telemetry, and Intelligenc. Trellix Advanced Research Center. Obtido em 27 de julho de 2025, de https://www.trellix.com/advanced-research-center/threat-reports/april-2025/

Tril, M. (27 de março de 2025). Russian propaganda network Pravda tricks 33% of AI responses in 49 countries. Euromaidan Press. Obtido em 27 de julho de 2025, de https://euromaidanpress.com/2025/03/27/russian-propaganda-network-pravda-tricks-33-of-ai-responses-in-49-countries/

Verhelst, K. (21 de julho de 2025). Putin is stepping up 'aggressive' hybrid attacks on Germany, spy chief warns. Politico. Obtido em 25 de julho de 2025, de https://www.politico.eu/article/vladimir-putin-aggressive-hybrid-attacks-germany-spy-chief-martina-rosenberg/

Vincent, E. (12 de julho de 2025). French army chief says Russia 'will pose a real threat before 2030'. Le Monde. Obtido em 21 de julho de 2025, de https://www.lemonde.fr/en/politics/article/2025/07/12/french-army-chief-says-russia-will-pose-a-real-threat-before-2030_6743302_5.html

Walker, C., & Ludwig, J. (2017). The meaning of sharp power: How authoritarian states project influence. Foreign affairs, 16(11).

Wallner, C., Copeland, S., & Giustozzi, A. (2025). Russia, AI and the Future of Disinformation Warfare - Emerging Insights. Royal United Services Institute for

Defence and Security Studies (RUSI). Obtido em 30 de julho de 2025, de https://static.rusi.org/russia-ai-and-the-future-of-disinformation-warfare.pdf

Wasinger, M., Lins, B., Bronk, C., Pijpers, P. B., Lehto, M., Papadaki, M., . . . Marahrens, S. (2024). Aspects of Cognitive Warfare. Defence Horizon Journal. Obtido em 22 de julho de 2025, de https://tdhj.org/wp-content/uploads/2024/11/2024_TDHJ-Hybrid-CoE-Cgnitive-Warfare-2024_web-v2.pdf

Wilson, E. J. (01 de março de 2008). Hard Power, Soft Power, Smart Power. The ANNALS of the American Academy of Political and Social Science, pp. 110-124. doi:10.1177/0002716207312618

Wood, M. (2013). International Law and the Use of Force: What Happens in Practice? Indian Journal of International Law, pp. 345-367. Obtido em 02 de abril de 2025, de https://legal.un.org/avl/pdf/ls/wood_article.pdf

World Economic Forum. (2024). The Global Risks Report 2024 - Insight Report. World Economic Forum (WEF). Obtido em 23 de julho de 2025, de https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

World Economic Forum. (15 de janeiro de 2025). Global Risks Report 2025: conflito armado, ambiente e desinformação são as prinicpais ameaças. Lisboa: World Economic Forum (WEF). Obtido em 23 de julho de 2025, de https://reports.weforum.org/docs/WEF_Global_Risks_Report_Press_Release_2025_PT.pdf

Zakaria, F. (30 de março de 2025). Russian philosopher: Putinism has won in the US. GPS. Obtido em 03 de abril de 2025, de https://edition.cnn.com/2025/03/30/world/video/gps0330-putin-russia-ukraine-dugin

Zelenskyy, V. (13 de abril de 2025). Ukrainian President Volodymyr Zelenskyy: The 2025 60 Minutes Interview transcript. 60 Minutes. (S. Pelley, Entrevistador) Obtido em 21 de abril de 2025, de https://www.cbsnews.com/news/ukraine-president-volodymyr-zelenskyy-2025-60-minutes-interview-transcript/