Guerra híbrida como coerção politicamente dirigida: tecnologia, ambiguidade e vulnerabilidade estratégica

Jorge M. Lasmar

Resumo

A guerra híbrida constitui uma forma contemporânea de coerção politicamente dirigida, na qual instrumentos militares e não militares são combinados para produzir efeitos estratégicos sob condições de ambiguidade. O artigo compara conceitos, autores e debates doutrinários a partir de uma abordagem qualitativa e teórico-conceitual, revendo conceitos sobre guerra híbrida, ambiguidade estratégica, tecnologia, fricção, vulnerabilidades sistêmicas, e o pensamento de Clausewitz. Sustenta-se que a guerra híbrida não representa uma essência inteiramente nova da guerra, mas um modo específico de integrar coerção, ambiguidade e exploração de vulnerabilidades. Sua eficácia depende da capacidade de intensificar incertezas, dificultar a atribuição de responsabilidade, retardar respostas e pressionar vulnerabilidades informacionais, institucionais, infraestruturais e sociais já existentes. Por fim, a tecnologia exerce papel central nas ameaças híbridas ao ampliar a escala, a velocidade, a opacidade e o alcance dessas ações, mas não substitui sua lógica política. Assim, a guerra híbrida pode ser compreendida como exploração coordenada de vulnerabilidades sob condições de ambiguidade.

Abstract

Hybrid warfare constitutes a contemporary form of politically directed coercion in which military and non-military instruments are combined to produce strategic effects under conditions of ambiguity. The article compares concepts, authors, and doctrinal debates through a qualitative and theoretical-conceptual approach, reviewing discussions on hybrid warfare, strategic ambiguity, technology, friction, systemic vulnerabilities, and Clausewitz's thought. It argues that hybrid warfare does not represent an entirely new essence of war, but rather a specific way of integrating coercion, ambiguity, and the exploitation of vulnerabilities. Its effectiveness depends on the ability to intensify uncertainty, complicate attribution of responsibility, delay responses, and pressure pre-existing informational, institutional, infrastructural, and social vulnerabilities. Finally, technology plays a central role in hybrid threats by expanding the scale, speed, opacity, and reach of these actions, but it does not replace their political logic. Thus, hybrid warfare can be understood as the coordinated exploitation of vulnerabilities under conditions of ambiguity.

Introdução

O conflito contemporâneo é cada vez mais conduzido por meio da combinação de ações cibernéticas disruptivas, campanhas de desinformação, atores por procuração, sabotagem, pressão econômica, manipulação jurídica e uso calibrado da força. Casos como a guerra na Ucrânia reforçaram a percepção de que o conflito frequentemente se desenrola por meio de instrumentos militares e não militares que operam de forma combinada, tornando menos nítidas as distinções convencionais entre guerra e paz, pressão interna e externa, e ação cinética e não cinética. No entanto, essa amplitude também pode tornar o conceito teoricamente impreciso. Este artigo aceita a crítica de que o termo guerra híbrida tem sido, por vezes, excessivamente elástico, mas não

conclui que seu uso deva ser abandonado. Ao contrário, argumenta que a guerra híbrida permanece analiticamente útil quando definida por sua lógica estratégica: o uso coordenado de instrumentos combinados para produzir efeitos políticos sob condições de ambiguidade.

Este artigo conecta três debates que frequentemente são tratados separadamente: a expansão excessiva do conceito de guerra híbrida, o problema clausewitziano do propósito político e do atrito, e a coerção tecnologicamente mediada como forma de exploração de vulnerabilidades. O argumento aqui apresentado é que a guerra híbrida deve ser compreendida não como um tipo inteiramente novo de guerra, mas como uma forma contemporânea de coerção politicamente dirigida. Seu caráter distintivo está na coordenação de instrumentos militares e não militares para explorar ambiguidades, intensificar incertezas e pressionar vulnerabilidades estrategicamente significativas sem necessariamente desencadear uma guerra interestatal aberta e em larga escala. A questão analítica central, portanto, não é apenas quais ferramentas são utilizadas, mas como essas ferramentas são integradas em torno de um propósito político.

Essa linha de análise é consistente com a visão clássica de que o conflito armado permanece subordinado ao propósito político, mesmo quando suas formas, ritmo e tecnologias mudam ao longo do tempo (Clausewitz, 1976). Ela também ressoa com a compreensão de Hoffman da guerra híbrida como a fusão de diferentes modos de conflito e com esforços mais recentes para identificar a ambiguidade como uma das características centrais do conceito (Hoffman, 2007; Mumford e Carlucci, 2023). Neste artigo, a ambiguidade não é tratada como a única característica definidora da guerra híbrida, mas como a condição estratégica que permite que instrumentos combinados dificultem a atribuição, tornem os limiares menos nítidos, fragmentem o consenso político e atrasem ou restrinjam as respostas (Mumford e Carlucci, 2023).

A tecnologia amplifica essa lógica, mas não a substitui. Sua importância está menos em criar uma nova lógica política do conflito do que em expandir a escala, a velocidade, o alcance, a opacidade e a persistên-

cia da ação coercitiva em múltiplos domínios. Infraestruturas digitais, comunicações em rede, capacidades cibernéticas, plataformas de informação, sensores comerciais e sistemas habilitados por IA tornam mais fácil, barato e, em alguns casos, mais plausivelmente negável perturbar sistemas, manipular percepções e pressionar vulnerabilidades que não podem ser reduzidas apenas a alvos no campo de batalha (Mumford e Carlucci, 2023). A tecnologia, portanto, funciona principalmente como facilitadora e multiplicadora da coerção híbrida, especialmente quando vulnerabilidades estratégicas estão localizadas na credibilidade informacional, coesão institucional, infraestrutura crítica e confiança pública.

O artigo está organizado em quatro seções. A primeira esclarece o conceito de guerra híbrida e identifica as principais tensões em torno de seu uso. A segunda examina o propósito político e explica por que a ambiguidade é estrategicamente útil na gestão da atribuição, retaliação e escalada. A terceira analisa como a mudança tecnológica intensifica a incerteza e o atrito em múltiplos domínios. A quarta desloca o foco dos instrumentos para as vulnerabilidades, argumentando que a guerra híbrida deve ser melhor entendida como a exploração coordenada de vulnerabilidades informacionais, institucionais, sociais e de infraestrutura.

1. Guerra híbrida em debate

A guerra híbrida continua sendo difícil de definir porque o termo tem sido usado para descrever diferentes fenômenos. As primeiras definições focaram na combinação de métodos militares convencionais e irregulares dentro de uma mesma campanha (Hoffman, 2007; Glenn, 2009). Abordagens doutrinárias e políticas posteriores ampliaram o conceito para incluir o uso coordenado de instrumentos militares e não militares em múltiplos domínios (OTAN, 2024).

A literatura mais recente tem enfatizado a ambiguidade, as operações cibernéticas, a desinformação, os atores por procuração (proxy) e a gestão de limiares como elementos centrais da coerção híbrida (Mumford e Carlucci, 2023). À medida que o termo se espalhou pelo

campo dos estudos estratégicos, doutrina de defesa e debate político, ele também se entrelaçou com conceitos adjacentes como ameaças híbridas, conflito de zona cinzenta, guerra cognitiva, guerra política e guerra societal virtual (Mazarr et al., 2019; Steen, 2025). O resultado é um debate marcado tanto pela relevância analítica quanto pela confusão conceitual (Solmaz, 2022; Libiseller, 2023).

Em uma das primeiras formulações do termo, Hoffman definiu ameaças híbridas como adversários que empregam simultaneamente e de forma adaptativa uma mistura combinada de armas convencionais, táticas irregulares, terrorismo e criminalidade (Hoffman, 2007). O ponto central não era listar os métodos em si, mas a afirmação de que esses métodos poderiam ser usados juntos dentro de um mesmo espaço de batalha e campanha. Hoffman, portanto, mudou o debate das distinções binárias entre guerra "regular" e "irregular" para a ideia de que adversários contemporâneos cada vez mais combinam o uso de modalidades que muitas vezes eram tratadas separadamente. Neste sentido, Glenn reconheceu que as categorias de guerra estavam se tornando menos estanques, mas questionou se o "conflito híbrido" merecia reconhecimento como uma categoria genuinamente nova, e não como um subconjunto ou variante da guerra irregular (Glenn, 2009). Esse ceticismo inicial é importante porque demonstra que a contestação sobre o conceito esteve presente desde o início do debate.

O conceito posteriormente se ampliou. O que inicialmente se referia principalmente à violência mista em ambientes operacionais passou a incluir operações cibernéticas, campanhas de desinformação, pressão econômica, interferência eleitoral, manipulação jurídica, uso coercitivo da migração, guerra por procuração e ataques à infraestrutura crítica. Essa ampliação explica a crescente relevância do conceito, mas também a preocupação de que ele se torne excessivamente elástico caso toda forma de hostilidade abaixo do limiar da guerra aberta seja simplesmente incorporada ao rótulo de guerra híbrida (Solmaz, 2022; Mumford e Carlucci, 2023). Essa ampliação do escopo foi reforçada à medida que o conceito migrou dos debates acadêmicos e militares para o campo das

políticas públicas de defesa e da doutrina. Os marcos da OTAN tratam ameaças híbridas como características centrais do ambiente de segurança contemporâneo, especialmente após 2014, quando o termo passou a estar intimamente associado ao comportamento russo na Crimeia e no leste da Ucrânia (Libiseller, 2023; OTAN, 2024). Essa adoção doutrinária teve um efeito ambivalente. Por um lado, reconheceu corretamente a complexidade multidomínio da coerção contemporânea, mas por outro, também incentivou o uso da guerra híbrida como uma categoria ampla de planejamento ao invés de um conceito analítico preciso.

Nesse sentido, a literatura crítica é essencial. Solmaz argumenta que o termo guerra híbrida foi levado além de seu contexto original e aplicado a casos que carecem de suas características essenciais (Solmaz, 2022). Almäng aborda o problema de forma diferente, examinando a natureza vaga do termo "guerra híbrida" como uma categoria situada entre paz e guerra (Almäng, 2019). Stoker e Whiteside vão além, argumentando que tanto o "conflito em zona cinzenta" quanto a "guerra híbrida" frequentemente prejudicam, em vez de aprimorar, o pensamento estratégico ao borrar as distinções entre guerra, paz e competição geopolítica (Stoker e Whiteside, 2020). Libiseller acrescenta que a difusão do conceito foi impulsionada não apenas pelo valor explicativo, mas também pela moda acadêmica e política após a popularização do termo pela OTAN em 2014 (Libiseller, 2023).

Essas críticas não devem ser descartadas. Um conceito que se expande demais acaba explicando muito pouco. No entanto, seria igualmente errado concluir que a guerra híbrida é analiticamente inútil. Interpretações mais contidas preservam o termo ao restringir seu escopo. Caliskan, por exemplo, argumenta que a guerra híbrida é mais útil quando tratada por meio da teoria estratégica do que como prova de uma forma radicalmente nova de guerra (Caliskan, 2019). Mumford e Carlucci desenvolvem essa linha de pensamento argumentando que a essência da guerra híbrida reside na ambiguidade, e não na mera combinação de instrumentos. Sua contribuição desloca o debate dos inventários de ferramentas para a lógica estratégica que torna essas ferramentas

eficazes em combinação: incerteza sobre atribuição, intenção, limiar e resposta (Mumford e Carlucci, 2023).

Em conjunto, o debate sugere que o conceito de guerra híbrida permanece útil apenas se for definido de modo suficientemente restrito para não se converter em sinônimo de qualquer conflito complexo ou não convencional. Na literatura, um conjunto limitado de elementos aparece repetidamente: a combinação de diferentes instrumentos de poder; a integração de meios militares e não militares; coordenação entre domínios; ambiguidade deliberada; direcionamento político, psicológico e social; e um esforço, ao menos inicialmente, para permanecer abaixo do limiar de uma guerra aberta e em larga escala (Hoffman, 2007; Solmaz, 2022; Mumford e Carlucci, 2023). Visto sob essa perspectiva, este artigo trata a guerra híbrida não como um novo tipo de guerra, mas como um modo contemporâneo de coerção integrada no qual atores estatais ou não estatais coordenam instrumentos militares e não militares para explorar a ambiguidade, aplicar pressão gradual e enfraquecer a capacidade do adversário de responder efetivamente. Cinco dimensões são especialmente importantes: integração instrumental, ambiguidade, gradualismo, direcionamento psicológico e social, e exploração sistêmica da vulnerabilidade. Definida dessa forma, a guerra híbrida permanece um conceito útil não porque nomeia tudo de novo sobre conflitos contemporâneos, mas porque captura uma lógica estratégica específica por meio da qual instrumentos mistos geram efeitos coercitivos cumulativos sob condições de ambiguidade (Caliskan, 2019; Hoffman, 2007; Mumford e Carlucci, 2023).

2. Propósito político e ambiguidade

O debate conceitual se torna mais claro quando a guerra híbrida é abordada a partir do propósito político, e não da sua suposta novidade. Clausewitz permanece indispensável aqui porque trata a guerra como um instrumento político e não como uma esfera autônoma de violência. Para ele, o objeto político é o motivo original da guerra e mol-

da tanto o objetivo militar quanto o grau de esforço a ser despendido (Clausewitz, 1976). Aplicado à guerra híbrida, isso significa que a questão analítica decisiva não é se operações cibernéticas, desinformação, proxies, sabotagem, pressão econômica, medidas legais ou força limitada estão presentes. É o efeito político que esses instrumentos pretendem produzir quando usados em conjunto. O argumento de Caliskan é útil precisamente por essa razão: a guerra híbrida é melhor abordada por meio da teoria estratégica do que tratada como uma nova categoria doutrinária (Caliskan, 2019). Mumford e Carlucci fazem um movimento semelhante ao argumentar que sua essência não está na novidade, mas na função política da ambiguidade (Mumford e Carlucci, 2023). Uma leitura clausewitziana, portanto, trata a guerra híbrida como uma configuração historicamente específica de coerção politicamente dirigida, em vez de uma ruptura com a teoria estratégica clássica. Guerra e coerção podem mudar em forma, ritmo e mediação tecnológica, mas permanecem subordinadas ao propósito político. Isso está alinhado com a afirmação de Caliskan de que a guerra híbrida não deve ser entendida como uma doutrina nova, e com a visão de Mumford e Carlucci de que ela é melhor vista como uma escolha operacional adequada à competição estratégica contemporânea do que como uma "nova guerra" (Caliskan, 2019; Mumford e Carlucci, 2023). A implicação chave é simples: a prioridade analítica deve ser o propósito, não a novidade.

Uma vez que o propósito político é priorizado, a atração estratégica dos métodos híbridos torna-se mais clara. Campanhas híbridas são frequentemente projetadas para garantir ganhos políticos limitados, mas significativos, sem incorrer nos custos de uma guerra aberta e em larga escala. Esses ganhos podem incluir enfraquecer a coesão do adversário, alterar gradualmente fatos no terreno, criar poder de barganha, moldar o ambiente político antes que um confronto armado mais amplo se torne necessário ou dividir internamente um país ou uma coalizão adversária. A discussão de Clausewitz sobre guerra limitada é relevante porque mostra que objetivos políticos menores podem exigir esforços menores. Isso também significa que o sucesso pode, em certos casos,

ser buscado por meio de efeitos políticos, e não apenas militares, como desarticular alianças ou paralisar a vontade do oponente (Clausewitz, 1976). A pesquisa contemporânea aponta na mesma direção: Mazarr define estratégias de zona cinzenta como campanhas graduais abaixo dos limiares que causariam uma escalada; Wigell conceitua a interferência híbrida como uma estratégia divisória; e Chivvis enfatiza que a guerra híbrida russa atua dentro dos marcos políticos e sociais existentes para avançar objetivos estratégicos, em vez de simplesmente destruir alvos militares (Mazarr, 2015; Wigell, 2019; Chivvis, 2017). Portanto, o conceito de guerra híbrida é mais útil quando visto como uma forma de coerção ajustada a propósitos políticos limitados e cuidadosamente calibrados.

Central para essa lógica política está a ambiguidade. Ambiguidade não é simplesmente vagueza ou ocultação; é uma condição estratégica em que o alvo enfrenta múltiplas interpretações plausíveis sobre atribuição, intenção, limiares e resposta adequada (Mumford e Carlucci, 2023). Para Mumford e Carlucci, esse é o elemento definidor da guerra híbrida porque força os defensores a agir sob incerteza, dispersando atenção e recursos entre cenários concorrentes. Sua utilidade não está apenas em obscurecer a responsabilidade, mas também em atrasar a tomada de decisões, complicar a retaliação, fragmentar o consenso interno e aliado, e permitir que atores revisionistas modulem a escalada. O conceito de negação plausível de Wigell aponta para o mesmo mecanismo, enquanto o trabalho de Mazarr sobre a zona cinzenta enfatiza a tentativa deliberada de permanecer abaixo das linhas vermelhas que possam desencadear uma resposta convencional (Wigell, 2019; Mazarr, 2015). Ao mesmo tempo, trabalhos recentes que distinguem a guerra híbrida da interferência híbrida abaixo do limiar do conflito armado são um lembrete útil de que nem toda coerção ambígua é guerra no sentido estrito (Bergaust e Sellevåg, 2024).

Clausewitz também ajuda a explicar por que a ambiguidade é eficaz. Sua teoria da guerra é estruturada em torno de atrito, incerteza, probabilidade, paixão e a dificuldade do julgamento em conflitos reais.

Uma leitura clausewitziana da guerra híbrida, portanto, não ficaria especialmente impressionada com a novidade das ferramentas cibernéticas, operações de informação, atores por procuração ou manipulação legal-política em si. O que importa é como esses instrumentos geram atrito dentro do sistema político e societal do oponente. Nesse sentido, a guerra híbrida pode ser entendida como uma forma de coerção que atua simultaneamente sobre as três tendências da notável trindade de Clausewitz. Primeiro, ela pressiona a esfera da razão e do governo ao complicar a atribuição, classificação legal, avaliações de proporcionalidade e gestão de escalada. Os tomadores de decisão são forçados a agir sob incerteza, muitas vezes sem evidências suficientes para construir consenso interno ou aliado para a resposta. Segundo, explora o acaso e a probabilidade multiplicando incidentes ambíguos, sinais incertos, atores cuja vinculação pode ser plausivelmente negada e interações contingentes entre os domínios cibernético, informacional, político, econômico e militar. O defensor deve interpretar se os eventos são isolados, coordenados, acidentais, criminosos, políticos ou militares, e esse ônus interpretativo aumenta a possibilidade de erro de cálculo. Terceiro, mobiliza a paixão ao atacar emoções públicas, desconfiança social, medo, humilhação, ressentimento e polarização. Campanhas de desinformação, sabotagem simbólica, sinalização coercitiva e violência por procuração podem inflamar divisões existentes e tornar as comunidades políticas menos capazes de julgamento coletivo. Como resultado, a guerra híbrida não é simplesmente uma mistura de instrumentos. É um modo de coerção que busca perturbar a relação entre razão política, incerteza e paixão social. Seu valor estratégico está em tornar o sistema político do adversário menos capaz de decidir, coordenar e responder de forma coerente. Nesse sentido, a ambiguidade não é apenas um véu que esconde a ação; é um mecanismo para converter a incerteza em instrumento de coerção sobre toda a comunidade política.

Ao mesmo tempo, uma análise clausewitziana alerta contra o excesso de extensão da linguagem da guerra. Nem todo ato hostil encoberto, plausivelmente negável ou situado abaixo do limiar da guerra aberta

deve ser classificado como guerra. Algumas atividades agrupadas sob o rótulo híbrido são melhor compreendidas como ação coercitiva de Estado, guerra política ou interferência híbrida conduzida abaixo do limiar do conflito armado (Wigell, 2019; Bergaust, e Sellevåg, 2024). Essa distinção não enfraquece o conceito; ela o aperfeiçoa. A guerra híbrida deve ser reservada para campanhas politicamente dirigidas nas quais instrumentos militares e não militares são coordenados para explorar ambiguidades, impor pressão gradual e enfraquecer a capacidade do adversário de resposta coerente sem necessariamente desencadear uma guerra aberta.

3. Tecnologia, incerteza e atrito

A combinação de métodos coercitivos associada à guerra híbrida não é nova. O que distingue o momento atual é o ambiente tecnológico no qual esses métodos são articulados, sincronizados e empregados. Redes digitais, capacidades cibernéticas, ecossistemas de informação plataformados, sistemas de IA, satélites comerciais e drones de baixo custo não alteram a natureza política do conflito. Em vez disso, alteram algumas de suas características operacionais, como velocidade, escala, alcance, precisão, opacidade e persistência. Em termos clausewitzianos, a tecnologia muda os meios e, portanto, o caráter prático do conflito, sem alterar o fato de que guerra e coerção permanecem subordinadas ao propósito político (Clausewitz, 1976). Assim, as tecnologias contemporâneas não inventam conflitos híbridos, mas expandem o repertório disponível de instrumentos, ampliam a possibilidade de explorar vulnerabilidades em sociedades complexas e possibilitam efeitos em múltiplos domínios com velocidade e persistência incomuns (Beyerchen, 1992; Thiele, 2020; Romansky et al., 2024).

É útil distinguir entre coerção híbrida dependente de tecnologia e coerção híbrida intensificada por tecnologia. A primeira refere-se a práticas hostis que dependem de infraestrutura digital ou sistemas técnicos avançados para existirem como táticas viáveis, como implantes

de malware, botnets de redes sociais, mídias sintéticas, personificação assistida por IA, intrusões cibernéticas em sistemas industriais de controle e falsificação de GPS. A segunda refere-se a práticas coercitivas mais antigas cuja eficácia é amplificada pelas tecnologias contemporâneas. A propaganda torna-se algoritmicamente direcionada e escalável; a vigilância torna-se automatizada e intensiva em dados; a sabotagem torna-se mais precisa; a coordenação de atores por procuração se torna mais rápida; e funções de reconhecimento e ataque se difundem por drones e sensores em rede comercialmente disponíveis. Essa distinção é importante porque a tecnologia reduz os custos de entrada para novos atores, aumenta a superfície de ataque e tanto cria novas formas de coerção quanto aprimora práticas antigas de subversão, engano, intimidação e disrupção.

Operações cibernéticas estão entre os exemplos mais claros de coerção híbrida habilitada pela tecnologia. Sua atração não reside apenas no potencial disruptivo, mas também na ambiguidade. A atribuição raramente é um fato puramente técnico; é um processo político pelo qual a incerteza é reduzida o suficiente para justificar a ação e atribuir significado a um incidente (Egloff e Dunn, Cavelty, 2021). É por isso que operações cibernéticas são úteis em campanhas híbridas: podem criar disrupções ao mesmo tempo em que permitem negação plausível, atraso e contestação sobre responsabilidade e intenção. No entanto, é importante evitar determinismo tecnológico. Borghard e Lonergan argumentam que efeitos cibernéticos ofensivos sofisticados são frequentemente ferramentas imperfeitas de coerção e escalada porque exigem acesso prévio, reconhecimento, exploits personalizados e condições favoráveis de direcionamento; mesmo assim, os efeitos permanecem incertos e frequentemente limitados (Borghard e Lonergan, 2017; Borghard e Lonergan, 2019). Essa advertência também ressoa com o argumento de Rid de que muitas atividades descritas como guerra cibernética são melhor entendidas como sabotagem, espionagem ou subversão do que como guerra no sentido estrito (Rid, 2012). Lindsay mostra de forma semelhante que a arquitetura interdependente do ciberespaço cria incentivos para

a contenção, mesmo enquanto permite uma competição persistente de baixo nível (Lindsay, 2017). Operações cibernéticas, portanto, são politicamente atraentes, mas seus efeitos estratégicos permanecem contingentes, incertos e frequentemente mais limitados do que relatos populares sugerem.

A inteligência artificial intensifica essa lógica ao acelerar a produção, o direcionamento, a circulação e a interpretação de efeitos coercitivos. Sua relevância para a guerra híbrida é especialmente visível no domínio informacional, em que sistemas generativos podem ampliar a escala, a velocidade, a personalização e a adaptabilidade linguística das operações de influência. Deepfakes, materiais audiovisuais manipulados, personas sintéticas e geração de conteúdo assistida por IA tornam a confiança em evidências digitais mais contestável e o engano mais escalável (Candolin et al., 2021; Hanhijärvi, 2026). No entanto, operações militares recentes também sugerem que a relevância da IA já não se limita à desinformação, às mídias sintéticas ou às operações de influência. Ela se torna cada vez mais visível na fusão de inteligência, no desenvolvimento de alvos e na aceleração dos ciclos de seleção de alvos. A Reuters relatou que o Pentágono utilizou ferramentas Claude, da Anthropic, durante ataques dos Estados Unidos ao Irã, embora não tenha conseguido determinar com precisão como essas ferramentas foram integradas ao esforço de guerra (Reuters 2026). A Chatham House também observou que o Almirante Brad Cooper confirmou o uso de ferramentas avançadas de IA para filtrar grandes volumes de dados e acelerar a tomada de decisão no conflito, ao mesmo tempo em que ressaltou que o grau de envolvimento da IA em decisões específicas de seleção de alvos permanecia sem confirmação (Amaral, 2026). Isso é importante porque a IA pode comprimir o tempo entre detecção, interpretação, designação de alvos, revisão jurídica e execução do ataque. Ela pode reduzir algumas formas de atrito operacional, mas desloca esse atrito para a qualidade dos dados, a supervisão humana, a revisão jurídica, a responsabilização e a compressão decisória. Sistemas de aprendizado de máquina são moldados por dados de treinamento, desenho de modelos e processos

inferenciais opacos; podem produzir inferências úteis, erros ou manipulações com igual velocidade (Thiele, 2020). Pesquisas sobre análise de campo de batalha habilitada por IA também indicam vulnerabilidade a dados enviesados, falsificações, interferências e envenenamento de dados, o que significa que tais sistemas podem automatizar erros tão facilmente quanto automatizam inferências úteis (Gardner, 2024). Portanto, a IA reduz o custo marginal de alguns efeitos coercitivos, mas não abole a incerteza. Ela a redistribui.

Sistemas autônomos e semiautônomos de baixo custo reproduzem esse mesmo padrão de forma mais concreta. A guerra na Ucrânia demonstrou que pequenos drones comerciais podem desempenhar funções de reconhecimento, aquisição de alvos e ataque de precisão por uma fração do custo e do ônus organizacional associados ao poder aéreo tradicional (Kunertova, 2023). Sua importância reside menos na sofisticação em si do que na difusão e na compressão de custos. Capacidades antes associadas a forças armadas avançadas agora podem ser improvisadas, adaptadas e empregadas em escala por Estados e, em alguns contextos, por atores por procuração ou grupos não estatais. Em ambientes híbridos, isso amplia a gama de atores capazes de realizar vigilância, intimidação, sabotagem e ataques de autoria plausivelmente negável contra alvos militares e civis. Ao mesmo tempo, a expansão desses sistemas impõe novos encargos defensivos, pois mais sinais precisam ser interpretados, mais plataformas de baixo custo precisam ser interceptadas e mais incidentes ambíguos precisam ser distinguidos do ruído rotineiro de fundo (Kunertova, 2023; Romansky et al., 2024).

O ponto central é melhor compreendido através do conceito de atrito. Novas tecnologias frequentemente prometem clareza, controle e velocidade. No entanto, como argumenta Gardner, elas reduzem algumas formas de atrito ao mesmo tempo em que amplificam outras ou introduzem atritos inteiramente novos (Gardner, 2024). A dependência da rede cria pontos ocultos de falha; a complexidade do software produz comportamento opaco do sistema; a rápida circulação de informações fortalece o engano; e líderes políticos que operam sob pressão da mídia

podem ser pressionados a responder antes que atribuição, intenção e proporcionalidade estejam adequadamente estabelecidas (Turell, Su e Boulanin, 2020). A implicação é que a tecnologia é central para a guerra híbrida não porque transcende a lógica política do conflito, mas porque fornece novas formas de fabricar confusão, explorar dependência, reduzir alguns custos operacionais e aumentar o ônus de decisão do adversário.

4. Vulnerabilidades estratégicas e instrumentos mistos

Com base na mudança analítica desenvolvida acima, esta seção desloca a análise da pergunta sobre quais ferramentas são utilizadas para a questão mais estratégica de quais vulnerabilidades são tomadas como alvo, por que elas importam politicamente e como instrumentos mistos são coordenados para explorá-las. Atores que conduzem campanhas híbridas geralmente não buscam a decisão imediata no campo de batalha ou a conquista territorial direta como seu primeiro objetivo. Mais frequentemente, eles buscam efeitos políticos limitados: enfraquecimento da governabilidade, atraso na resposta, fragmentação de alianças, erosão da legitimidade, alteração de cálculos custo-benefício ou remodelação do ambiente em que a coerção posterior pode ocorrer. O conceito de centro de gravidade de Clausewitz permanece útil aqui porque direciona a atenção para as fontes de poder e de coesão do oponente (Clausewitz, 1976). Em campanhas híbridas contemporâneas, essas fontes frequentemente estão não apenas nas forças armadas, mas também na coesão política, integridade informacional, confiabilidade infraestrutural e capacidade institucional. A guerra híbrida, portanto, visa tanto o funcionamento de uma comunidade política quanto seu aparato militar (Mumford e Carlucci, 2023; Jungwirth et al., 2023; Wrange, 2026).

Isso ajuda a explicar por que o direcionamento psicológico, político e social é central para a guerra híbrida. O objetivo muitas vezes é menos persuadir populações inteiras do que aprofundar divisões já existentes, amplificar a desconfiança e reduzir a capacidade de ação política cole-

tiva. O conceito de Wigell de interferência híbrida como uma "estratégia de divisão" (*wedge strategy*) captura essa dinâmica: atores externos exploram a abertura liberal por meio da diplomacia clandestina, geoeconomia e desinformação para dividir sociedades-alvo e enfraquecer a governabilidade (Wigell, 2019). A análise de Paul e Matthews sobre a "mangueira de incêndio da falsidade" russa mostra de forma semelhante que volume, repetição e inconsistência podem ser eficazes não porque produzem crenças coerentes, mas porque sobrecarregam a atenção, corroem a confiança na verificação e confundem julgamentos (Paul e Matthews, 2016). Mazarr et al. estendem esse argumento sugerindo que a "guerra societal virtual" tem como alvo a confiança, a estabilidade social e o funcionamento das sociedades democráticas, e não apenas as capacidades militares (Mazarr et al., 2019). Trabalhos empíricos recentes reforçam o ponto: operações de influência frequentemente buscam alcance entre comunidades já polarizadas ou marginais, explorando divisões que já existiam antes do próprio ataque (Okholm, 2025).

Essas dinâmicas importam porque as sociedades contemporâneas funcionam cada vez mais como sistemas densamente conectados em rede. Infraestrutura crítica, plataformas digitais, cadeias logísticas, sistemas de mensagens financeiras, serviços em nuvem, redes de comunicação e ambientes de informação eleitoral são profundamente interdependentes. Essa interdependência é relevante porque a densidade dos fluxos transnacionais pode amplificar a sensibilidade e a vulnerabilidade dos sistemas sociais, econômicos, logísticos e institucionais, produzindo efeitos em cascata que ultrapassam rapidamente o setor inicialmente afetado (Lasmar e Santa Rita, 2021). O conceito de interdependência instrumentalizada como arma, desenvolvido por Farrell e Newman, mostra como os atores podem explorar posições centrais nessas redes para vigilância, coerção e disrupção (Farrell e Newman, 2019). Uma lógica semelhante aparece nos marcos de resiliência da União Europeia, que tratam ameaças híbridas como pressões sistêmicas capazes de explorar dependências e gerar efeitos em cascata entre domínios cívicos, de governança e de serviços (Jungwirth et al., 2023). Vulnerabilidade estratégica, portanto, não

significa mais apenas exposição militar na fronteira. Ela também inclui dependência digital, fragilidade institucional, concentração de infraestrutura, desconfiança pública, dependência da cadeia de suprimentos, assimetrias legais e polarização política. Muitos desses elementos pertencem a sistemas civis com relevância militar direta, razão pela qual os debates contemporâneos sobre resiliência enfatizam cada vez mais a colaboração civil-militar e a preparação para toda a sociedade, em vez de apenas a defesa militar estrita (Willmer, 2023; Wrange, 2026).

O valor estratégico dos instrumentos mistos reside em sua capacidade de operar sobre essas vulnerabilidades. Campanhas híbridas raramente dependem de um único ato decisivo. Elas combinam intrusões cibernéticas, operações de influência, proxies, sabotagem, pressão econômica, manipulação legal e sinalização militar calibrada de maneiras que se reforçam mutuamente ao longo do tempo. Robinson et al. definem tais campanhas como usos deliberados de múltiplos instrumentos de poder para afetar a tomada de decisão sem recorrer à guerra convencional aberta (Robinson et al., 2018). Na interferência híbrida, a desinformação frequentemente é acompanhada de pressão geoeconômica e influência política encoberta ou semi-encoberta (Wigell, 2019). Operações cibernéticas também podem contribuir para essa orquestração, não apenas por meio de efeitos técnicos diretos, mas também por consequências de segunda ordem para instituições, alinhamentos de elite e atitudes públicas. Nesse sentido, influência eficaz requer moldar o ambiente informacional, não apenas hackear sistemas ou contas (Whyte, 2020; Whyte e Etudo, 2025). A guerra híbrida opera por meio de sequenciamento, reforço e acumulação: o que importa não são as ferramentas em si, mas sua integração estratégica em torno de vulnerabilidades exploráveis.

Isso também ajuda a explicar por que métodos híbridos contemporâneos podem oferecer alavancagem estratégica seletiva para estados mais fracos, proxies e alguns atores não estatais. A digitalização reduz os custos de certas capacidades disruptivas. Ferramentas cibernéticas, comportamento inautêntico coordenado, sabotagem remota e operações de

influência baseadas em plataformas podem impor sérios encargos sem exigir paridade nas forças convencionais (Willmer, 2023). No entanto, esses métodos não eliminam a hierarquia da política internacional. Sua eficácia depende do acesso, preparação, capacidade organizacional e das vulnerabilidades subjacentes ao alvo. Maschmeyer está certo ao alertar que operações cibernéticas enfrentam trade-offs entre velocidade, intensidade e controle, que limitam sua utilidade estratégica independente (Maschmeyer 2021). É por isso que campanhas híbridas dependem de combinações em vez de substituições. Operações de sabotagem, interrupção cibernética e influência tornam-se mais consequentes quando combinadas com outros instrumentos que exploram a confusão, desconfiança e desempenho degradado que criam dentro de sistemas complexos (Rovner, Cormac e Maschmeyer 2025). Métodos híbridos não tornam atores mais fracos iguais aos mais fortes, mas podem permitir efeitos desproporcionalmente disruptivos sob condições favoráveis.

Definida dessa forma mais restrita, a guerra híbrida permanece útil porque captura uma lógica estratégica específica. Essa lógica começa com a identificação de vulnerabilidades politicamente relevantes, como confiança, legitimidade, coesão, interoperabilidade, infraestrutura crítica e ciclos de decisão, e prossegue por meio do uso coordenado de instrumentos mistos para explorá-los cumulativamente sob condições de ambiguidade. Nem todo ciberataque, campanha de desinformação ou episódio de diplomacia coercitiva constitui guerra híbrida. O termo é valioso analiticamente apenas quando tais ações são integradas a uma campanha politicamente direcionada, projetada para enfraquecer a capacidade de resposta do adversário, mantendo a escalada incerta e contestada, e a atribuição de responsabilidade difícil de estabelecer claramente (Mumford e Carlucci, 2023; Jungwirth et al., 2023).

Conclusão

A guerra híbrida é melhor compreendida como uma forma de coerção historicamente específica, mediada tecnologicamente e politi-

camente dirigida, e não como uma essência totalmente nova da guerra. Sua importância contemporânea não reside na mera combinação de ferramentas militares e não militares, já que métodos mistos de coerção são historicamente recorrentes. Tampouco está apenas na novidade das operações cibernéticas, da inteligência artificial, dos drones, da desinformação ou dos atores por procuração. Esses instrumentos importam, mas não definem sozinhos a guerra híbrida. O que dá valor analítico ao conceito é a lógica estratégica pela qual diferentes instrumentos são coordenados para buscar efeitos políticos sob condições de ambiguidade.

Essa lógica possui três componentes centrais. Primeiro, a guerra híbrida permanece subordinada ao propósito político. Seus métodos são atraentes porque permitem que os atores busquem ganhos políticos limitados, porém significativos, enquanto gerenciam os riscos de atribuição, retaliação e escalada. Segundo, a ambiguidade não é incidental à guerra híbrida. É um de seus principais mecanismos. Ao obscurecer responsabilidade, intenção, limiares e resposta proporcional, a ambiguidade atrasa a tomada de decisão, fragmenta o consenso e aumenta o ônus de interpretação do defensor. Terceiro, a tecnologia intensifica essa lógica ao expandir a velocidade, escala, alcance, opacidade e persistência da ação coercitiva. Infraestruturas digitais, manipulação habilitada por IA, operações cibernéticas, sensores comerciais e drones de baixo custo não aboliram a incerteza; antes, a redistribuem e frequentemente criam novas formas de atrito.

A implicação mais importante é que a guerra híbrida deve ser analisada menos como um catálogo de ferramentas e mais como uma estratégia de exploração de vulnerabilidades. Comunidades políticas contemporâneas dependem de redes densas de confiança, informação, infraestrutura, logística, finanças e coordenação institucional. Esses sistemas são frequentemente civis em sua forma, mas estrategicamente decisivos em sua função. Campanhas híbridas exploram precisamente essas interdependências. Seus efeitos são cumulativos, e não necessariamente decisivos: um incidente cibernético pode reforçar uma operação

de influência; sabotagem pode aprofundar a desconfiança pública; manipulação legal pode atrasar a resposta; pressão econômica pode dividir coalizões; sinalização militar calibrada pode fazer a retaliação parecer custosa demais ou incerta.

Essa definição mais rígida também protege o conceito do uso excessivo. Nem toda operação cibernética hostil, campanha de desinformação, ação encoberta ou medida diplomática coercitiva deve ser chamada de guerra híbrida. O termo é mais útil quando se refere a campanhas politicamente direcionadas que coordenam instrumentos mistos para explorar a ambiguidade e enfraquecer a capacidade do adversário de responder de forma coerente. Nesse sentido, a guerra híbrida não substitui a teoria estratégica clássica. Ela confirma uma das percepções centrais da teoria estratégica clássica: o conflito pode mudar em forma, ritmo e tecnologia, mas continua organizado em torno do propósito político, da incerteza e do esforço de impor a própria vontade a um adversário.

Referências

ALMÄNG, Jan. War, Vagueness and Hybrid War. **Defence Studies** 19 (2), p. 189–204, 2019.

AMARAL, Nilza. **The Iran War Highlights the Creeping Use of AI in Warfare**. Chatham House, March 27, 2026.

BERGAUST, Julie Celine, and SELLEVÅG, Stig Rune. Improved Conceptualising of Hybrid Interference below the Threshold of Armed Conflict. **European Security** 33 (2), p. 169–195, 2024.

BEYERCHEN, Alan. 1992. Clausewitz, Nonlinearity, and the Unpredictability of War. **International Security** 17 (3), p. 59–90, 1992.

BORGHARD, Erica D., and LONERGAN, Shawn W.. The Logic of Coercion in Cyberspace. **Security Studies** 26 (3), p. 452–481, 2017.

BORGHARD, Erica D., and LONERGAN, Shawn W.. 2019. Cyber Operations as Imperfect Tools of Escalation. **Strategic Studies Quarterly** 13 (3), p. 122–145, 2019.

CALISKAN, Murat. Hybrid Warfare through the Lens of Strategic Theory. **Defense & Security Analysis** 35 (1), p. 40–58, 2019.

CANDOLIN, Catharina; CARVIN, Stephanie; CUSUMANO, Eugenio; LASCONJARIAS, Guillaume; LINDSTRÖM, Lauri; MYATT, Madeleine; SAVOLA, Reijo; WIJERMARS, Mariëlle; SMITH, Hanna; SCHROEFL, Josef; LAPPALAINEN, Emma, and VÄLIMÄKI, Jarno. The Future of Cyberspace and Hybrid Threats. **Hybrid CoE Trend Report** 6. Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2021.

CHIVVIS, Christopher S. **Understanding Russian "Hybrid Warfare":** And What Can Be Done About It: Addendum. Santa Monica, CA: RAND Corporation, 2017.

CLAUSEWITZ, Carl von. **On War**. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press,1976.

EGLOFF, Florian J., and Myriam Dunn CAVELTY. 2021. Attribution and Knowledge Creation Assemblages in Cybersecurity Politics. **Journal of Cybersecurity** 7 (1), 2021.

FARRELL, Henry, and Abraham L. NEWMAN. Weaponized Interdependence: How Global Economic Networks Shape State Coercion. **International Security** 44 (1), p. 42–79, 2019.

GARDNER, Nikolas. Clausewitzian Friction and Twenty-First-Century War—The Paradox of Technology. **Naval War College Review** 77 (1), 2024.

GLENN, Russell W. Thoughts on 'Hybrid' Conflict. **Small Wars Journal**, March 3, 2009.

HANHIJÄRVI, Heidi. Artificial Intelligence and Foreign Information Manipulation: Chinese and Russian Approaches. **Hybrid CoE Paper** 29. Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2026.

HOFFMAN, Frank G. **Conflict in the 21st Century:** The Rise of Hybrid Wars. Arlington, VA: Potomac Institute for Policy Studies, 2007.

JUNGWIRTH, Rainer, SMITH, Hanna; WILLKOMM, Etienne; SAVOLAINEN, Jukka; VILLOTA, Marina Alonso; LEBRUN, Maxime; AHO, Aleksi; and GIANNOPOULOS, Georgios. **Hybrid Threats:** A Comprehensive Resilience Ecosystem. Luxembourg: Publications Office of the European Union, 2023.

KUNERTOVA, Dominika. Drones Have Boots: Learning from Russia's War in Ukraine. **Contemporary Security Policy** 44 (4), p. 576–591, 2023.

LASMAr, Jorge M., and SANTA RITA, Leonardo Coelho Assunção. Coronavirus, Global Risk and The New International Crisis Management Model. **Conjuntura Internacional** 17 (3), p. 47–61, 2021.

LIBISELLER, Chiara. Hybrid Warfare as an Academic Fashion. **Journal of Strategic** *Studies* 46 (4), p. 858–880, 2023.

LINDSAY, Jon R. Restrained by Design: The Political Economy of Cybersecurity. **Digital Policy, Regulation and Governance** 19 (6), p. 493–514, 2017.

MASCHMEYER, Lennart. The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. **International Security** 46 (2), p. 51–90, 2021.

MAZARR, Michael J. **Mastering the Gray Zone:** Understanding a Changing Era of Conflict. Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press. https://press.armywarcollege.edu/monographs/428/, 2015.

MAZARR, Michael J.; BAUER, Ryan M.; CASEY, Abigail; HEINTZ, Sarah A.; MATTHEWS, Luke J. **The Emerging Risk of Virtual Societal Warfare:** Social Manipulation in a Changing Information Environment. Rand: Santa Monica, 2019.

MUMFORD, Andrew, and Pascal CARLUCCI. Hybrid Warfare: The Continuation of Ambiguity by Other Means. **European Journal of International Security** 8 (2), p. 192–206, 2023.

NATO. **Hybrid Threats and Hybrid Warfare Reference Curriculum**. Brussels: NATO / Partnership for Peace Consortium, 2024.

OKHOLM, Christiern Santos. Conditions of Subversive Reach: Comparing Societal and Strategic Factors for Russian Propaganda Outlets' Reach among Western European Fringe Communities. **European Journal of International Security**, First View, p. 1–23, 2025.

PAUL, Christopher, and MATTHEWS, Miriam. **The Russian "Firehose of Falsehood" Propaganda Model:** Why It Might Work and Options to Counter It. Santa Monica, CA: RAND Corporation, 2016.

REUTERS. **US Uses Anthropic AI, B-2 Bombers and Suicide Drones in Iran Strikes**. March 2, 2026.

RID, Thomas. Cyber War Will Not Take Place. **The Journal of Strategic Studies** 35 (1), p. 5–32, 2012.

ROBINSON, Linda, HELMUS, Todd C.; COHEN, Raphael S.; NADER, Alireza; RADIN, Andrew; MAGNUSON, Madeline; and MIGACHEVA, Katya. **Modern Political Warfare:** Current Practices and Possible Responses. Santa Monica, CA: RAND Corporation, 2018.

ROMANSKY, Sofia, HOENIG, Alisa; MEESSEN, Rick; and KRUIJVER, Kimberley. **New Technologies, Changing Strategies:** Five Trends in the Hybrid Threat Landscape. The Hague: The Hague Centre for Strategic Studies and TNO, 2024.

ROVNER, Joshua; CORMAC, Rory, and MASCHMEYER, Lennart. Sand in the Gears: Sabotage in World Politics. **European Journal of International Security**, p. 1–20, 2025.

SOLMAZ, Tarık. 'Hybrid Warfare': A Dramatic Example of Conceptual Stretching. National Security and the Future 23 (1), p. 9–30, 2022.

STEEN, B. J. M. Søndergaard. **Cognitive Warfare**, 2025.

STOKER, Donald, and WHITESIDE, Craig. Blurred Lines: Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking. **Naval War College Review** 73 (1), p. 12–48, 2020.

THIELE, Ralph. **Artificial Intelligence – A Key Enabler of Hybrid Warfare**. Hybrid CoE Working Paper 6. Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2020.

TURELL, Johan; SU, Fei, and BOULANIN, Vincent. Cyber-Incident Management: Identifying and Dealing with the Risk of Escalation. **SIPRI Policy Paper** 55. Stockholm: Stockholm International Peace Research Institute, 2020.

WHYTE, Christopher, and ETUDO, Ugochukwu. Finding the Thieves amongst the Liars: Thinking Clearly about Cyber-Enabled Influence Operations. **European Journal of International Security**, p. 1–19, 2025.

WHYTE, Christopher. Beyond Tit-for-Tat in Cyberspace: Political Warfare and Lateral Sources of Escalation Online. **European Journal of International Security** 5 (2), p. 195–214, 2020.

WIGELL, Mikael. 2019. Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy. **International Affairs** 95 (2), p. 255–275.

WILLMER, Lukas. Does Digitalization Reshape the Principle of Non-Intervention? **German Law Journal** 24 (Special Issue 3), p. 508–521, 2023.

WRANGE, Jana. Strategic Autonomy: A 'Quantum Leap Forward on' European Total Defence? **European Journal of International Security**, First View, p. 1–22, 2026.

Jorge M. Lasmar é Coordenador do Programa de Pós-Graduação em Relações Internacionais da PUC Minas e Professor Colaborador do Mestrado em Ciências Policiais e Tecnologias Inovadoras da Academia da Polícia Militar de MG. É doutor em Relações Internacionais pela London School of Economics, LSE, e atua como consultor para diversas organizações internacionais, com ampla experiência na capacitação de forças policiais, militares, de inteligência e instituições públicas.