



A inteligência artificial e o nevoeiro da guerra: a dissonância entre automação e incerteza

*Artificial intelligence and the
fog of war: the dissonance between
automation and uncertainty*

*La inteligencia artificial y la
niebla de la guerra: la disonancia entre
automatización e incertidumbre*

DOI: 10.21530/ci.v20n3.2025.1586

Thiago José Bandeira Santos¹

Rachel Camilly Soares de Souza²

Copyright:

• This is an open-access article distributed under the terms of a Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided that the original author and source are credited.

• Este é um artigo publicado em acesso aberto e distribuído sob os termos da Licença de Atribuição Creative Commons, que permite uso irrestrito, distribuição e reprodução em qualquer meio, desde que o autor e a fonte originais sejam creditados.



Resumo

O uso crescente da inteligência artificial no campo militar tem despertado reflexões sobre como essa tecnologia poderia mudar a forma como lidamos com as incertezas da guerra. Este artigo analisa a influência da inteligência artificial sobre o conceito clausewitziano de “nevoeiro da guerra”, considerando as transformações nos conflitos contemporâneos, com ênfase na guerra entre Rússia e Ucrânia. A partir de uma abordagem qualitativa, conclui-se que, embora a inteligência artificial contribua para a compressão dos ciclos decisórios e a ampliação da consciência situacional, essa tecnologia não elimina a incerteza inerente à guerra, ao contrário, a reconfigura.

Palavras-chave: Inteligência Artificial, Névoa de Guerra, Sistemas autônomos, Tomada de Decisão, Clausewitz.

1 Doutorando em Ciências Militares pela Escola de Comando e Estado-Maior do Exército (ECEME). (t.bandeirapqdt@gmail.com). ORCID: <https://orcid.org/0000-0003-1797-1383>.

2 Mestranda em Ciências Militares pela Escola de Comando e Estado-Maior do Exército (ECEME). (rachelcamillyss@gmail.com). ORCID: <https://orcid.org/0009-0004-1888-0218>.

Artigo submetido em 01/06/2025 e aprovado em 12/11/2025.





Abstract

The increasing use of artificial intelligence in the military field has sparked reflections on how this technology could transform the way we deal with the uncertainties of war. This article analyzes the influence of artificial intelligence on the Clausewitzian concept of the “fog of war,” taking into account the transformations in contemporary conflicts, with a particular focus on the war between Russia and Ukraine. Adopting a qualitative approach, the study concludes that, although artificial intelligence contributes to the compression of decision-making cycles and the enhancement of situational awareness, it does not eliminate the uncertainty inherent to war; on the contrary, it reconfigures it.

Keywords: Artificial Intelligence, Fog of War, Autonomous systems, Decision-Making, Clausewitz.

Resumen

El uso creciente de la inteligencia artificial en el ámbito militar ha suscitado reflexiones sobre cómo esta tecnología podría transformar la manera en que enfrentamos las incertidumbres de la guerra. Este artículo analiza la influencia de la inteligencia artificial sobre el concepto clausewitziano de la “niebla de la guerra”, considerando las transformaciones en los conflictos contemporáneos, con énfasis en la guerra entre Rusia y Ucrania. A partir de un enfoque cualitativo, se concluye que, aunque la inteligencia artificial contribuye a la comprensión de los ciclos decisorios y a la ampliación de la conciencia situacional, esta tecnología no elimina la incertidumbre inherente a la guerra; por el contrario, la reconfigura.

Palabras clave: Inteligencia Artificial, Niebla de la guerra, Sistemas autónomos, Toma de decisiones, Clausewitz.

1 Introdução

O atual ambiente de mudanças geopolíticas e rápido desenvolvimento de soluções baseadas em Inteligência Artificial (IA) estão alterando o setor de defesa (Semenenko et al. 2025). Nesse sentido, as principais implicações militares da IA permitem o seu emprego no desenvolvimento de sistemas autônomos, na consciência situacional avançada e em novas tecnologias de uso dual. O primeiro se refere aos sistemas que podem operar sem controle humano direto, como “bots”, drones e veículos terrestres ou navais. O segundo se trata de segurança cibernética, guerra de informações e sistemas de tomada de decisão assistida. Os





últimos se vinculam à melhoria da performance em setores civil-militar, como as áreas de logística, pessoal e de saúde (Lindsay 2023).

A inteligência artificial constitui um campo amplo e multidisciplinar, não podendo ser reduzida a uma única técnica. Conforme Russell e Norvig (2016), a IA pode ser definida como a evolução de sistemas de computador capazes de executar tarefas que normalmente exigiriam inteligência humana racional, envolvendo reconhecimento de fala, tomada de decisões e solução de problemas. Para esses autores existem quatro categorias em que a IA pode ser definida: (i) sistemas que imitam seres humanos; (ii) sistemas que raciocinam como indivíduos; (iii) sistemas que refletem de maneira racional, (iv) sistemas que comportam-se de maneira racional. Os softwares que imitam indivíduos exibem comportamento semelhante ao humano.

Para tal feito, a ferramenta precisa ter habilidades específicas, como processamento de linguagem natural, representação de conhecimento, argumentação automatizada e aprendizado de máquina, o que possibilita a adaptação a novas eventualidades e a extrapolação da competência no cenário atual (Russell e Norvig 2016). Dessa forma, a IA abrange desde sistemas que imitam comportamentos humanos até aqueles que raciocinam e agem de maneira racional. Esse estudo entende a inteligência artificial como uma ferramenta ampla, capaz de integrar diversos métodos e tecnologias com vistas a solucionar problemas complexos. Assim sendo, a inteligência artificial possui utilidade em múltiplos domínios, como reconhecimento de padrões, automação de processos de comando e controle, apoio à tomada de decisão, segurança cibernética e planejamento estratégico na defesa, reforçando seu caráter abrangente.

Nesse escopo, o desenvolvimento de sistemas baseados em IA necessita de um grande volume de dados fidedignos para o treinamento das máquinas. Isso é uma realidade no mundo corporativo que segue as normas do estado de direito (Lindsay 2023). Contudo, a guerra é a atividade humana mais vinculada ao acaso e se caracteriza por eventos inesperados e imprevisíveis (Paret, Howard e Brodie 1984), sendo um desafio adicional para o treinamento das máquinas.

Clausewitz na sua obra *Da Guerra* (1832) apresenta diversos conceitos que moldaram o pensamento estratégico moderno. Entre esses conceitos, a “névoa da guerra” se destaca como uma das imagens mais duradouras para explicar a incerteza e a complexidade que permeiam os conflitos armados. A névoa da guerra é uma metáfora para os desafios cognitivos, informacionais e emocionais enfrentados pelos decisores e combatentes, tendo uma significativa relevância nos conflitos da atualidade (Paret, Howard e Brodie 1984).





Argumenta-se que as inovações tecnológicas criadas no século XX levaram estrategistas a questionar a lógica clausewitziana, pois havia uma tendência a acreditar que a superioridade tecnológica removeria a “névoa da guerra” do campo de batalha (Murray 1997). Contudo, o incremento da ciência e tecnologia no campo militar não levou a esse desfecho, mas aumentou a dependência de sistemas de informação (Lindsay 2023). Esses debates reacenderam com o emprego da IA no campo de batalha e se tornaram pontos cruciais para as estratégias de defesa dos países (Wyatt 2024). A partir desse cenário de crescente importância da IA e da constante incerteza que se vincula a natureza da guerra, depreende-se o seguinte problema de pesquisa: de que modo a IA influencia o “nevoeiro da guerra” nos conflitos contemporâneos?

De modo a responder esse questionamento, este estudo realiza uma abordagem qualitativa entre os conceitos clássicos presentes no livro “a natureza da guerra” de Clausewitz (Paret, Howard e Brodie 1984) à luz de artigos de Doutrina Militar que abordam as influências da IA nos combates da atualidade, como Kania (2019) e Johnson (2022). Ademais, a pesquisa adota como estudo de caso, o conflito entre Rússia e Ucrânia (2022–presente), escolhido por reunir condições singulares para observação, como o emprego extensivo de sistemas autônomos, o uso sistemático de algoritmos de apoio à decisão e a integração entre operações cibernéticas e ações cinéticas (Zysk 2024).

Reconhece-se, entretanto, que o uso de fontes abertas e jornalísticas pode gerar riscos de viés informacional, sobretudo em um ambiente de guerra caracterizado por campanhas de desinformação e censura seletiva. Ademais, a ausência de acesso a dados classificados restringe o detalhamento de certas dimensões operacionais, limitando a completude da análise. Outro viés potencial decorre da predominância de perspectivas ocidentais na literatura e nos relatórios consultados, o que pode introduzir uma leitura assimétrica do conflito. Embora essas limitações imponham cautela na generalização dos resultados, o estudo oferece contribuições teóricas e empíricas relevantes, capazes de gerar *insights* para o debate sobre automação, incerteza e a evolução da natureza da guerra no século XXI.

2 O nevoeiro da guerra na era digital

Clausewitz compreendia a guerra como uma atividade profundamente humana e, portanto, sujeita a falhas de percepção, julgamentos errôneos e interferências





emocionais. Nesse escopo, “a guerra é o domínio da incerteza. Três quartos dos fatores em que baseiam se os combates na guerra estão envoltos numa névoa de maior ou menor incerteza” (Paret, Howard e Brodie 1984, 109). Essa afirmação torna-se central para entender como Clausewitz concebia a natureza essencialmente imprevisível da guerra, desafiando modelos simplistas ou mecanicistas de análise estratégica. O ambiente de conflito se desenrola em meio à penumbra, na qual a incerteza tende a distorcer a percepção dos fatos, fazendo com que eventos e ameaças pareçam mais amplos ou mais graves do que são realmente.

A névoa da guerra aparece em sua obra interligada a outros conceitos fundamentais, como fricção e golpe de vista (*coup d’œil*). A fricção diz respeito ao conjunto de atividades imprevistas que se acumulam mesmo quando aparentemente pequenas e podem comprometer o sucesso de uma operação. Clausewitz afirmou ainda que: “A fricção é o único conceito que contém mais ou menos os fatores que distinguem a guerra real da guerra no papel” (Paret, Howard e Brodie 1984, 132). De outra forma, o golpe de vista refere-se à capacidade intuitiva do comandante de perceber, em meio à névoa, as oportunidades e os riscos com clareza, mesmo diante de informações incompletas. Para o autor, essa habilidade constitui um dos atributos essenciais para lidar com o imprevisto (Paret, Howard e Brodie 1984).

A metáfora da névoa descreve a dificuldade de perceber a realidade da guerra. Ao contrário de jogos de xadrez, em que todas as peças são visíveis, na guerra real grande parte das informações estão ausentes, deturpadas ou divergentes. Clausewitz observou que: “Na guerra, muitos relatórios de inteligência são contraditórios; outros, em número ainda maior são falsos e a maioria é precária” (Paret, Howard e Brodie 1984, 129). Portanto, a guerra impõe um desafio constante ao raciocínio lógico e exige uma forma de julgamento que transcende a análise puramente racional. Assim sendo, o “nevoeiro da guerra” é a união de diversos elementos que caracterizam os conflitos armados, como a incerteza, o acaso, a fricção e o caos. Em termos gerais, a guerra envolve aspectos que não podem ser completamente conhecidos ou previstos, sendo inevitável a presença de certo grau de ambiguidade (Creveld 1985).

O pensamento estratégico estadunidense após a Guerra do Vietnã, buscou uma transformação nesse entendimento por meio da emergência de uma nova cultura militar marcada pela crença na superioridade tecnológica como instrumento para superar as incertezas da guerra (Murray 1997). Essa transformação conceitual se insere no contexto da chamada Revolução nos Assuntos Militares (RAM), que





passa a reconfigurar o aparato tecnológico das forças armadas, suas doutrinas, estruturas organizacionais e formas de conceber a guerra (Murray e Knox 2022). Como argumenta Wyatt (2024), a RAM representa uma mudança em que campo de batalha é reconceituado como um ambiente interconectado, guiado por dados e informações em tempo real, no qual a capacidade de decisão veloz e precisa se sobrepõe à força bruta tradicional. Nesse novo cenário, a guerra passa a ser percebida como um sistema integrado de fluxos informacionais, em que sensores, IA e redes de Comando e Controle (C2) operam de forma coordenada para produzir uma superioridade cognitiva sobre o inimigo. A promessa tecnocrática de dissolver a fricção e a incerteza ganha força à medida que se acredita que os avanços tecnológicos podem suprimir os elementos imprevisíveis do combate (Murray 1997).

Entretanto, Murray e McMaster alertam para os riscos dessa abordagem tecnocrática da guerra, que tende a reduzir o fenômeno bélico a uma operação puramente técnica, previsível e gerenciável. Segundo esses autores, tal visão ignora dimensões fundamentais, políticas, culturais e humanas, que moldam os conflitos armados. McMaster (2009), ao analisar os equívocos estratégicos cometidos pelos Estados Unidos no Vietnã, Afeganistão e Iraque, argumenta que essa perspectiva mecanicista obscureceu a compreensão da natureza política dos conflitos, a identidade dos oponentes e os fatores endógenos que estruturam o campo de batalha. Ambos defendem que a guerra, em sua essência, permanece um fenômeno humano, permeado por fricções, ambiguidades e incertezas que não podem ser eliminadas por sensores, algoritmos ou plataformas tecnológicas, por mais avançadas que sejam as tecnologias empregadas nos conflitos (Murray 1997; McMaster 2009).

A ampliação da capacidade de coleta e disseminação de dados no campo de batalha não erradica a incerteza inerente à guerra; ao contrário, apenas a transfere para outras esferas da estrutura decisória. Conforme argumenta Martin van Creveld (1985), a informação não possui um efeito puramente redutor sobre a névoa da guerra. Pelo contrário, o acúmulo massivo de dados pode sobrecarregar os tomadores de decisão e gerar novas formas de ambiguidade, retardando respostas estratégicas e táticas. Nesse sentido, a incerteza não é superada pela tecnologia da informação, mas deslocada, muitas vezes obscurecendo ainda mais a compreensão situacional dos comandantes.

No plano teórico, estudiosos como Lawrence Freedman (2013) e Colin Gray (1999) têm enfatizado que a guerra, mesmo sob as condições da modernidade





tecnológica, permanece essencialmente uma atividade humana, marcada por incertezas estruturais, ambiguidades interpretativas e conflitos de interesse. Freedman, ao conceber a estratégia como uma construção narrativa, argumenta que os estrategistas atuam em contextos de profunda instabilidade, sendo compelidos a projetar o futuro a partir de dados fragmentários, em ambientes permeados por pressões políticas, institucionais e cognitivas (Freedman 2013). Nessa direção, a estratégia não é um produto de cálculo técnico, mas um processo contingente de formulação de sentido frente à complexidade do real. Para Gray (1999), a guerra não pode ser compreendida como uma operação mecânica ou como uma simples aplicação de técnicas gerenciais, mas como uma prática historicamente informada, sujeita a paixões, erros de julgamento, choques de percepção e jogos de poder. Quando considerados em conjunto, Freedman e Gray oferecem uma crítica contundente à racionalidade instrumental, reafirmando a centralidade da incerteza, da interpretação e da contingência como fundamentos constitutivos da guerra e da estratégia em qualquer época.

Sob a ótica dos Estudos de Ciência e Tecnologia, Lucy Suchman (2007) oferece uma das críticas mais sofisticadas a essa visão tecnodeterminista ao argumentar que sistemas de guerra autônomos não são instrumentos neutros, mas artefatos sociotécnicos inscritos em redes de valores, protocolos institucionais e práticas culturais. Sua análise da guerra de *drones* revela que a promessa de “precisão cirúrgica” é uma construção retórica, em grande medida, pois os sistemas de vigilância e ataque são mediados por operadores humanos, por processos de categorização que podem falhar e por interpretações situadas de dados sensoriais. Tal perspectiva desloca o debate de uma visão puramente técnica para uma análise sociopolítica, demonstrando que cada decisão algorítmica está embutida em um ecossistema de atores, normas e relações de poder. Essa contribuição é crucial para repensar a fricção clausewitziana no século XXI em que o erro não é apenas um resíduo a ser eliminado, mas um produto da interação entre humanos, máquinas e instituições.

Aplicada ao campo militar, essa abordagem expõe que conceitos como “consciência situacional”, isto é capacidade de observar compreendendo elementos em um ambiente operacional e prever seu estado futuro para tomar decisões, não são meramente técnicos, mas também políticos, pois envolvem decisões sobre o que medir, quais ameaças priorizar e quais riscos aceitar (Latour 1991). Atualmente, essa dinâmica reconfigura a fricção clausewitziana se manifestando em disputas sobre responsabilidade legal e governança algorítmica. Nesse contexto, outro





conceito é o de *trading zones* que mostra o desenvolvimento de tecnologias de guerra como um processo de tradução entre comunidades epistêmicas (cientistas, engenheiros, militares), cada uma com seus códigos e prioridades, sendo um processo repleto de potenciais ruídos e mal-entendidos que adicionam novas camadas de fricção (Galison 1994).

Para Bousquet (2009) cada era tecnológica gera uma epistemologia da guerra e demonstra que o ideal de consciência situacional total é inalcançável. Na era da guerra em rede, a interconexão cria novas vulnerabilidades: sobrecarga informacional, risco de falhas em cascata e superfícies ampliadas para ataques cibernéticos. A análise é reforçada pela constatação de que infraestruturas de segurança produzem simultaneamente visibilidade e invisibilidade, convertendo grandes volumes de dados em ruído, o que requer interpretação crítica. Essa dinâmica dialoga diretamente com a advertência de Clausewitz de que a informação no campo de batalha é frequentemente contraditória e fragmentada, exigindo cuidadosa avaliação para a tomada de decisão estratégica (Bellanova 2021).

A competição por supremacia em IA no contexto militar não elimina a necessidade de julgamento humano, uma vez que sistemas baseados em aprendizado de máquina permanecem vulneráveis a ataques adversariais, falhas de generalização e vieses ocultos. Um falso positivo em sistemas de alerta precoce pode desencadear escaladas involuntárias de conflito, aumentando os riscos estratégicos em vez de reduzi-los. Dessa forma, a fricção clausewitziana não desaparece na guerra contemporânea, mas se transforma. Esses incidentes inesperados incluem falhas de software, mau funcionamento de sensores, desinformação algorítmica, ataques cibernéticos de negação de serviço e dilemas éticos mediados por sistemas opacos. Portanto, o ambiente resultante possui maior complexidade, exigindo doutrinas adaptativas, redundância técnica e mecanismos de governança capazes de lidar com a opacidade e o risco inerentes a essas tecnologias emergentes (Scharre 2024).

Logo, a reconfiguração do “nevoeiro da guerra” deve ser compreendida como fenômeno sociotécnico. Clausewitz permanece essencial para entender a persistência da incerteza, mas a literatura apresentada demonstra que a tecnologia não dissipa o caos; ela o redistribui e, em certos casos, o intensifica. Assim sendo, a crítica ao tecnodeterminismo é indispensável para evitar soluções simplistas e para promover arquiteturas de decisão resilientes, supervisionadas e preparadas para operar no caos.





De que forma o advento da IA altera esse diagnóstico crítico sobre a relação entre tecnologia e o nevoeiro da guerra? No relatório do *Center for a New American Security* desenvolvido por Work e Grant (2019), a IA e a autonomia podem comprimir os ciclos decisórios ao ponto em que a cognição humana se torna um fator limitante, potencialmente reduzindo fontes tradicionais de atrito. Os autores destacam aplicações práticas em logística e reconhecimento, mas igualmente enfatiza a necessidade de manter humanos no ciclo decisório para contextos que exigem julgamento moral e estratégico. Assim sendo, a IA poderia permitir um grau de velocidade e precisão na tomada de decisões que altera o caráter fundamental da guerra, embora a imprevisibilidade persista em ambientes complexos (Kania 2019).

A análise das perspectivas otimistas fundamentadas revela que a IA representa um avanço revolucionário na gestão do nevoeiro da guerra, embora dentro de limites claros. Como demonstram Scharre (2018) e Brose (2020), a IA oferece capacidades inéditas para comprimir ciclos decisórios, processar informações em tempo real e reduzir erros humanos, fatores que tradicionalmente alimentavam a fricção e a incerteza clausewitzianas. A capacidade de sistemas autônomos para “penetrar o nevoeiro” (Scharre 2018) ou conceder “vantagens decisivas” (Brose 2020) aponta para uma transformação genuína na condução de conflitos. No entanto, Brose adverte que essa transparência crescente não é absoluta, visto que, sistemas de IA podem criar novas vulnerabilidades e pontos de falha, mantendo elementos de imprevisibilidade. Para Husain (2017), a IA pode mitigar o atrito ao tomar decisões na velocidade das máquinas, mas a imprevisibilidade humana e as falhas intencionais ou não nos modelos de aprendizagem das máquinas sempre terão papel na guerra. Esta visão reflete um consenso entre especialistas: enquanto a IA transforma aspectos fundamentais da guerra, elementos clausewitzianos como fricção, acaso e incerteza não desaparecem, mas sim se manifestam de novas formas.

Contudo, como os próprios autores enfatizam, essa transformação não equivale à eliminação do nevoeiro da guerra. A imprevisibilidade humana (Husain 2017), as vulnerabilidades técnicas (Brose 2020) e a persistência de ambientes complexos (Kania 2019) mantêm relevância estratégica. A IA não suprime a natureza fundamentalmente caótica da guerra, mas a reconfigura, deslocando o nevoeiro do domínio da informação bruta para desafios mais sutis, como a confiabilidade algorítmica, a guerra cognitiva e a resiliência de sistemas automatizados. Logo, no campo dos estudos estratégicos e da segurança internacional, o conceito de





névoa da guerra permanece um referencial teórico relevante para a compreensão de conflitos.

3 Inteligência artificial no campo de batalha

O conceito de “névoa da guerra”, permanece uma lente central para compreender os dilemas da guerra contemporânea. Clausewitz enfatiza que a tomada de decisão no campo de batalha é marcada pela informação incompleta, incerteza e fricção. A “fricção”, conceito-chave em sua obra, designa a força invisível que transforma o simples (Clausewitz 2010). Nas últimas décadas, a rápida transformação tecnológica, com o advento de sensores em rede, *big data*, sistemas de comando e IA, levaram a especulação sobre a possibilidade de “dissipar” a névoa da guerra, reduzindo drasticamente a fricção. Entretanto, uma análise, inspirada nos Estudos de Ciência e Tecnologia (STS) e na teoria crítica de segurança, mostra que essa expectativa é tecnodeterminista e insuficiente. Em vez de eliminar a incerteza, a tecnologia frequentemente a redistribui, criando novas zonas de opacidade, novos riscos e novas fricções sociotécnicas.

Diante disso, a IA no campo de batalha contemporâneo está reconfigurando paradigmas operacionais e estratégicos, gerando intensos debates sobre seu impacto na natureza da guerra (Scharre 2018). Longe de ser um avanço monolítico, a IA manifesta-se em diversas aplicações que merecem análise distinta. Para organizar essa discussão, o restante da seção visou a abordagem dos seguintes eixos centrais: o debate estratégico sobre sistemas autônomos e a corrida armamentista; a transformação dos processos de Comando e Controle; a intensificação das campanhas cibernéticas e de informação; e a otimização da logística militar. Por meio dessa estrutura foi possível conectar os avanços tecnológicos diretamente aos desafios clausewitzianos de fricção, incerteza e tomada de decisão sob pressão.

3.1 Sistemas autônomos, riscos estratégicos e a nova corrida armamentista

Um dos debates mais proeminentes sobre a IA militar gira em torno do desenvolvimento de sistemas de armas autônomas e suas consequências geopolíticas (Scharre 2018). O uso de IA no campo de batalha tem sido objeto de intensos debates entre teóricos das relações internacionais, estudiosos de segurança internacional e engenheiros de sistemas bélicos. Por exemplo, Paul





Scharre e Michael Horowitz reconhecem o potencial da IA para transformar o combate moderno, mas divergem quanto aos riscos e à governança necessária para lidar com os efeitos dessa mudança.

Em *Army of None*, Scharre (2018) defende que a autonomia deve ser tratada com cuidado, particularmente no que diz respeito à tomada de decisões letais. Esse autor argumenta que os sistemas autônomos não são inerentemente antiéticos, mas que, sem uma supervisão humana rigorosa e sem salvaguardas robustas, a tecnologia pode tomar decisões erradas. Sua preocupação com os sistemas letais autônomos se concentra na dificuldade de responsabilização em casos de erro e na erosão da autoridade humana no campo de batalha. A preocupação de Scharre dialoga diretamente com a “fricção” de Clausewitz, sugerindo que falhas algorítmicas ou vieses nos dados podem introduzir novas formas de atrito, com consequências fatais.

Por outro lado, Horowitz (2019) foca nas consequências geopolíticas, alertando que a velocidade de decisão impulsionada pela IA pode reduzir as chances de desescalada em crises, alimentando a instabilidade estratégica global. Essa perspectiva destaca como a tecnologia, ao tentar superar a “névoa da guerra” pela velocidade, pode paradoxalmente aumentar o risco de escaladas inadvertidas, um fator desestabilizador em um ambiente de incerteza.

Essa dinâmica alimenta uma nova corrida armamentista, protagonizada por Estados Unidos e China, que investem maciçamente em IA para redefinir os parâmetros de segurança e defesa (Weshues 2025). A IA torna-se um ativo estratégico que amplia a capacidade de dissuasão e influência global. Essa competição não apenas acelera o desenvolvimento de sistemas autônomos, mas também levanta preocupações éticas sobre a perda progressiva do controle humano, criando uma “lacuna de responsabilização” quando uma máquina tira uma vida, um dilema à luz do Direito Internacional Humanitário (Weshues 2025; Santayana 2024; Zysk 2024; Wyatt 2024).

3.2 Comando e Controle: aceleração e vulnerabilidades no Ciclo OODA

Outro fator a ser considerado na incorporação da IA ao campo de batalha contemporâneo tem sido a transformação dos processos de Comando e Controle, particularmente no que tange à tomada de decisão. Uma das estruturas conceituais mais importantes para entender essas mudanças é o ciclo Observar, Orientar, Decidir e Agir (OODA), proposto pelo Coronel da Força Aérea dos Estados Unidos





John Boyd. Este processo ocorre de maneira contínua de modo que um agente (individual ou organizacional) coleta informações, interpreta-as, decide e executa uma ação (Boyd 2007).

De acordo com Boyd (2007), a superioridade em combate advém dessa capacidade de realizar o ciclo OODA mais rapidamente do que o adversário, desestabilizando sua capacidade de reação e impondo uma vantagem estratégica que permita a manutenção da iniciativa durante o combate. Assim, o agente que pode manipular a sua orientação e decidir mais rapidamente em face de uma situação ambígua e em rápida mudança dominará o ambiente de combate. Neste contexto, a IA aparece como uma tecnologia capaz de acelerar consideravelmente esse ciclo, especialmente nas fases de observar e orientar em que a coleta e a interpretação de dados são cruciais.

A capacidade da IA de processar vastos volumes de dados em tempo real representa um avanço sem precedentes na fase de observação do ciclo OODA. As plataformas de reconhecimento baseadas em visão computacional, aprendizado profundo e análise de sinais podem processar imagens de satélite, comunicações interceptadas e outras fontes de inteligência com velocidade e acurácia superiores às capacidades humanas. Isso reduz significativamente o tempo de latência entre o surgimento de um evento no teatro de operações e sua identificação pelos tomadores de decisão (Daniels 2021).

Na fase de orientação que envolve o enquadramento e a interpretação dos dados de observação com base em modelos mentais, doutrinas, experiência prévia e contexto cultural; a IA tem demonstrado potencial (Johnson 2022). Nesse contexto, a IA generativa pode fornecer múltiplos cenários de curso de ação, oferecendo ao comandante opções estratégicas com análise de risco embutida. Salienta-se que essa tecnologia se refere a aplicação da previsão estatística automatizada que cria conteúdo, como texto, código de software e design gráficos (Lindsay 2023).

Nas fases decidir e agir existe um debate significativo sobre a conveniência de delegar à IA a decisão final em situações letais. Como destaca Scharre (2018), a velocidade não pode substituir a responsabilidade. Em muitos casos, o tempo de pensar é justamente o tempo necessário para tomar decisões morais. Além disso, a transição para um ciclo OODA acelerado por IA pode paradoxalmente reduzir a margem de manobra estratégica, ao induzir uma “pressão de tempo” artificial.

Contudo, a aceleração do ciclo OODA introduz novas vulnerabilidades. Nas fases de Decidir e Agir, a delegação de decisões letais à IA é controversa.





Como aponta Scharre (2018), a velocidade não pode substituir a responsabilidade, e o “tempo de pensar” é crucial para decisões morais. A pressão por decisões rápidas pode comprometer a qualidade do julgamento humano, aumentando o risco de escaladas automatizadas (Daniels 2021). Isso ilustra uma reconfiguração da “névoa da guerra”, pois a incerteza não desaparece, mas se desloca da falta de dados para a dificuldade de validar as recomendações de sistemas algorítmicos opacos, gerando novas fricções sociotécnicas (Clausewitz 2010; Scharre 2024).

3.3 Campanhas cibernéticas e guerra de informação

A IA tem atuado ativamente nas campanhas cibernéticas. Essas integram um conjunto de operações coordenadas que visam objetivos distintos ao longo do tempo. As principais formas de ciberoperações são ataques cibernéticos e desinformação, pois visam causar perturbação, negação, degradação ou destruição de ameaças existentes ou potenciais, possibilitando atingir resultados que permitam uma vantagem estratégica imediata ou de longo prazo (Harknett e Smeets 2020). Essas funcionalidades da IA permitem que um Estado execute esse tipo de campanha no nível global, interferindo na dinâmica entre atores estatais. Dessa forma, a IA tem se tornado uma ferramenta central em campanhas cibernéticas, que integram ataques e desinformação para alcançar vantagens estratégicas com baixos efeitos colaterais visíveis. Essas operações visam perturbar, degradar ou destruir ameaças, permitindo que um Estado interfira na dinâmica global de forma encoberta (Harknett e Smeets 2020; Lopes 2021).

Nesse escopo, os sistemas de IA são empregados para automatizar a previsão de ataques, analisar tráfego de rede para identificar anomalias e fortalecer a cibersegurança (Semenenko et al. 2025). Contudo, a mesma tecnologia é usada para fins ofensivos, como a criação de *deepfakes* e a disseminação de desinformação por meio de *bots* em redes sociais, manipulando a opinião pública e enfraquecendo adversários (Lopes 2021). Portanto, esse domínio representa uma nova faceta da “névoa da guerra”, no qual a distinção entre verdade e falsidade se torna turva. Nesse escopo, a implementação de IA em cenários de combate não está isenta de desafios, sendo um de seus maiores riscos, o viés de automação.

Esse conceito se trata de um fenômeno cognitivo amplamente documentado na literatura, especialmente nos estudos sobre interação humano-máquina em contextos de decisão crítica. Skitka, Mosier e Burdick (1999) foram pioneiros na





definição desse viés, descrevendo-o como a tendência de indivíduos favorecerem sugestões automatizadas e ignorarem informações contrárias, mesmo que estas sejam mais precisas. Segundo os autores, o viés manifesta-se de duas formas: erros de comissão, quando o usuário aceita automaticamente a recomendação incorreta da máquina; e erros de omissão, quando o operador falha em agir porque a automação não forneceu nenhuma indicação (Skitka, Mosier e Burdick 1999).

Parasuraman e Riley (1997) também alertam que sistemas altamente precisos tendem a induzir complacência, diminuindo o monitoramento humano e a capacidade crítica do operador. Em contextos militares, essa precisão exacerbada pode comprometer a eficácia da decisão e aumentar o risco de consequências indesejadas, sobretudo em situações de ambiguidade, sobrecarga informacional ou pressão temporal. Assim, o viés de automação representa uma das principais limitações cognitivas associadas à integração da IA como ferramenta de apoio à decisão no campo de batalha.

Scharre (2018) argumenta que a capacidade de processamento avançado de sensores e algoritmos de reconhecimento de padrões permitem discriminar entre combatentes e não combatentes com margens de erro significativamente menores do que as alcançadas por operadores humanos sob pressão. Contudo, críticos como Lindsay (2023) alertam que a suposta precisão da IA é desenvolvida pela qualidade dos dados, que muitas vezes refletem vieses históricos ou contextos operacionais limitados.

Outrossim, o uso de reconhecimento facial em zonas de guerra tem levantado preocupações éticas e operacionais, com impactos documentados em diversos contextos. Estudos, como de Buolamwini e Gebru (2018), demonstraram que os sistemas de reconhecimento facial frequentemente apresentam vieses raciais, sendo menos precisos na identificação de rostos não brancos, uma falha crítica quando aplicada em operações militares. Como destacado por Brose (2020), a combinação entre identificação automatizada e ação militar pode levar a erros irreversíveis, especialmente quando os algoritmos não são suficientemente precisos ou transparentes em seu funcionamento. Nesse cenário, Scharre (2018) alerta que a automação acelera o tempo de reação mas também aumenta o risco de escaladas inadvertidas, especialmente na ausência de supervisão humana direta.

Do exposto, o viés de automação e a tendência humana de confiar excessivamente em sistemas automatizados agravam o problema, pois operadores podem aceitar informações falsas geradas por IA ou ignorar dados corretos se não forem validados pela máquina, comprometendo a tomada de decisão. Assim, a





IA não apenas explora a incerteza existente, mas ativamente a produz, tornando a guerra informacional um campo de batalha tão crítico quanto o físico.

3.4 Logística militar

No campo logístico, a IA oferece avanços notáveis para mitigar a “fricção” clausewitziana (Paret, Howard e Brodie 1984). Segundo Kott e Linkov (2019), os algoritmos de aprendizado de máquina podem prever falhas em cadeias de suprimento, redirecionar fluxos logísticos em tempo real e mitigar riscos de colapsos operacionais. Essas funcionalidades permitem melhorar a capacidade de sobrevivência, a eficácia e a eficiência das atividades de logística militar, permitindo o racionamento de militares em tarefas monótonas e perigosas. Ademais, a IA tem sido empregada no setor produtivo da indústria de defesa, reduzindo o papel do fator humano nas linhas de produção. Isso ocorre por meio do controle automático da qualidade de peças de componentes críticos, como o setor de aviação; na fabricação de motores, produção de testes simulados, dentre outras possibilidades (Zysk 2024).

No entanto, a dependência crescente de sistemas logísticos automatizados cria novas vulnerabilidades. Essas redes podem se tornar alvos prioritários em operações de guerra cibernética, suscetíveis à manipulação e sabotagem (Lindsay 2023). Portanto, embora a IA possa reduzir a fricção logística tradicional, ela também introduz novas complexidades e riscos, exigindo que a tecnologia seja vista como um amplificador das capacidades humanas e não como um substituto para o julgamento crítico (Kott e Linkov 2019).

4 A complexidade da Guerra entre Rússia e Ucrânia

Após o estudo teórico sobre o nevoeiro da guerra na era digital e da IA no campo de batalha, o conflito armado entre Rússia e Ucrânia emerge como um estudo de caso fundamental. Essa beligerância oferece condições singulares para observar empiricamente o emprego de novas tecnologias, como sistemas autônomos, permitindo uma compreensão da interação entre inovação tecnológica, fricção e tomada de decisão. Desse modo, essa guerra contemporânea se torna um laboratório prático para observar como a IA não dissolve, mas reconfigura a incerteza clausewitziana.





Nesse contexto, a Rússia, durante a fase de preparação da guerra, passou a empregar ferramentas de tomada de decisão e análise de dados, gerando uma enorme quantidade de dados que possibilitaram aos analistas de inteligência dos Estados Unidos, com meses de antecedência, concluir que ocorreria a ofensiva de Moscou sobre Kiev. Esses dados foram processados com auxílio de IA e permitiram a Ucrânia se preparar para a guerra, impedindo o elemento surpresa por parte da Rússia (Santayana 2024).

Nesse escopo, a desinformação russa não obteve sucesso no início da invasão, ocasião na qual a Rússia utilizou um vídeo falso, com técnicas de *deepfake*, em que o presidente ucraniano chamava os integrantes de seu país à rendição, tendo alcançado mais de 120 mil visualizações no Youtube (Santayana 2024). Em paralelo, a Rússia, nas primeiras cinco semanas do conflito, realizou massivamente campanhas no domínio cibernético, com cerca de 800 ataques contra alvos ucranianos. Essas atitudes ofensivas foram minimizadas por meio de uma combinação de esforços de defesa cibernética da Ucrânia e aliados ocidentais (Zysk 2024).

Logo, a vantagem estratégica de Kiev se baseou na sua precisa consciência situacional. Essa capacidade foi obtida por meio de diferentes sistemas baseados em IA (Santayana 2024). Dentre esses, a plataforma Delta consolida informações de diferentes fontes, incluindo militares, civis e drones. Esses dados possibilitam o planejamento das operações militares, a coordenação dos movimentos das tropas amigas e a identificação da localização de soldados e equipamentos inimigos (Goncharuk 2024). Esse sistema exemplifica como a integração de múltiplas fontes de dados são processadas com mais rapidez e precisão do que seria humanamente possível (Scharre 2018). Ao fornecer uma imagem unificada do campo de batalha, o Delta comprime as fases de “Observar” e “Orientar” do ciclo OODA (Boyd 2007), desempenhando papel fundamental na destruição do cruzador russo “Moskva” em abril de 2022 (Goncharuk 2024). Logo, a superioridade estratégica da Ucrânia decorreu da integração tecnológica e cognitiva promovida pela plataforma Delta, cuja capacidade de unificar e processar dados em tempo real ampliou a consciência situacional, acelerou o ciclo decisório e demonstrou como a inteligência artificial redefine o equilíbrio operacional em contextos de guerra contemporânea.

Outrossim, o *software* MetaConstellation fornecido pela Palantir abrange dados de sensores como: satélites, redes sociais (Santayana 2024), provedores civis fornecidos por multinacionais e empresas ucranianas (Onderco 2025) e





serviços de inteligência estrangeiros. Esses possibilitam a análise das operações de combate, o planejamento estratégico e o gerenciamento do campo de batalha. Assim, os ucranianos se utilizaram desses dados para realizar ataques precisos de longo alcance às tropas russas, retomando o controle da cidade de Kherson, em novembro de 2022 (Goncharuk 2024). Ao integrar fontes abertas, como redes sociais, com dados militares classificados, o sistema amplia a capacidade de observação e permite a identificação de padrões que seriam invisíveis de outra forma. Contudo, essa interconexão cria novas vulnerabilidades, como previsto por Bousquet (2009), transformando empresas privadas de tecnologia em alvos militares e gerando uma nova “fricção” logística e de segurança. Nesse sentido, a Rússia tem realizado ataques cibernéticos contra diversas empresas privadas que estão auxiliando nesse tipo de solução em IA pela Ucrânia (Onderco 2025).

Somado a isso, o sistema de consciência situacional *Kropyva* gerencia a informação de sensores, permitindo a seleção e priorização de alvos (Onderco 2025), bem como o suporte de fogos por meio de cálculos balísticos quando combinada com sistemas, como o GISArta que caracteriza-se por ser um tipo de sistema de Comando e Controle para fogo de Artilharia (Goncharuk 2024). O sistema *Kropyva* evidencia o papel da automação no apoio ao fogo de artilharia, acelerando cálculos e reduzindo erros humanos (Onderco 2025). Nesse caso, a névoa da guerra se reconfigura, pois a incerteza não está mais na falta de dados sobre o alvo, mas na confiança depositada nos algoritmos de priorização e nos cálculos do sistema (Clausewitz 2010; Scharre 2024). Um erro de software ou um dado corrompido pode levar a consequências fatais, exemplificando a “*moral crumple zone*”, em que a responsabilidade por uma falha algorítmica pode recair sobre o operador humano (Elish 2016).

Do exposto, a consciência situacional quando alinhada à tomada de decisão constitui um componente crítico para o sucesso nas operações militares. Nesse sentido, o desenvolvimento de Comando, Controle, Comunicações, Computadores, Inteligência, Vigilância e Reconhecimento (C4ISR) permite obter e manter a superioridade da informação. Essas funcionalidades se tornam mais precisas com o emprego da IA para coletar e analisar grandes quantidades de dados, tomando decisões rápidas que superem o adversário. Nessa direção, a Rússia integra essa capacidade aos seus meios militares por meio do Sistema *Informatsionnaya Sistema Boevogo Upravleniya* (ISBU) (Zysk 2024).

Além disso, a Rússia interrompe e degrada as comunicações, infraestrutura crítica, satélites e outras redes das quais a Ucrânia e seus aliados dependem,





a fim de impedir ou dificultar a superioridade da informação pelo oponente (Zysk 2024). Em oposição, os ucranianos empregam o software desenvolvido pela empresa norte-americana Primer. Essa solução utiliza o Processamento de Linguagem Natural para analisar as comunicações nas rádios russas (Santayana 2024). Essa abordagem evita que militares ucranianos demorem horas decifrando manualmente conversas interceptadas, processando rapidamente grandes volumes de dados derivados de rádios inimigas (Goncharuk 2024).

No que tange a proteção de infraestruturas críticas, a Ucrânia tem avançado na análise e classificação automática de ameaças, bem como tem combatido engenharia social russa que gera acessos a esses sistemas, como *deepfake*. Isso ocorre por meio de sistemas de detecção automática de *bots*, IA generativa inimiga e fontes de desinformação, bem como pelo desenvolvimento de ferramentas capazes de interagir com humanos por meio de voz, imagem, texto e vídeo. Nesse sentido, a Ucrânia monitora e analisa o espaço de informações com a plataforma analítica *Mantis* que permite detectar desinformação (Goncharuk 2024).

Outra possibilidade é o software de reconhecimento facial *Clearview* que foi treinado com base em fotografias retiradas de redes sociais. Essa tecnologia permite a identificação de soldados russos vivos e mortos, possibilitando agilidade nos informes públicos e integração da informação com outras capacidades, como guerra eletrônica, campanhas cibernéticas e criptografia (Santayana 2024). Destaca-se que a precisão desses sistemas é questionável, especialmente em condições de combate, bem como seus processos de treinamento que podem possuir vieses raciais ou de dados; resultando em identificações equivocadas com potenciais consequências letais (Buolamwini, Gebru 2018). Além disso, a empresa *Artellance* desenvolveu redes neurais para busca de perfis faciais, análise de texto e algoritmos para estruturação e limpeza de grandes volumes de dados que resultaram em vantagens sobre a desinformação russa (Goncharuk 2024).

Em paralelo, a defesa da Ucrânia identificou que os soldados russos frequentemente utilizam redes de telecomunicações tradicionais para contatar seus familiares e amigos. Diante disso, a empresa ucraniana Primer modificou seu software de transcrição de voz para processar chamadas interceptadas de militares russos de forma instantânea, auxiliando no processamento, seleção e geração de informações úteis para as Forças Armadas. O setor de defesa ucraniano também desenvolve aplicativos e Chatbots padronizados que permitem ao público alertar as autoridades militares sobre a localização exata de russos.



Essas ferramentas também são utilizadas pela Rússia que se utiliza de chamadas falsas para induzir militares ucranianos a ligarem para seus familiares, possibilitando a identificação das tropas e posterior ataque de artilharia (Onderco 2025). Outra forma de ataque russo é o sistema RB109-A Bylina que coleta grande quantidade de dados e por meio da IA prioriza e bloqueia os sinais eletrônicos (Zysk 2024). Essa frequência das ações ofensivas de Guerra Eletrônica dificultam a efetividade do “*human in the loop*” no conflito, priorizando a utilização de armas com sistemas autônomos baseados em IA (Goncharuk 2024). Esses meios envolvem a navegação autônoma e o planejamento de caminhos em todos os domínios (Weshues 2025).

Nessa classe estão incluídos os *Unmanned Ground Vehicle* (UGV), também denominados veículos terrestres não tripulados, como os robôs TALON que atuam no manuseio de artefatos químicos, biológicos, radiológicos, nucleares e explosivos, reduzindo os riscos para os soldados ucranianos. Cabe ressaltar que a solução TALON pode ser convertida em robô de combate (Westhues 2025). Por outro lado, a Rússia está avaliando o UGV Marker em combate real. Esse projeto russo possui Processamento de Linguagem Natural, Visão Computacional, navegação, movimento autônomo e controle de veículos em grupo (Santayana 2024). Ademais, a Rússia possui veículos não tripulados no domínio marítimo, como o Vityaz'd de submersão profunda e o veículo subaquático Poseidon que se move a energia nuclear e possui capacidade nuclear (Zysk 2024).

Além disso, a navegação autônoma pode ser utilizada para “*Loitering munition*”, também conhecidas como drones kamikazes. Esse sistema aéreo do tipo “dispare e esqueça” possui um alto grau de autonomia na busca por alvos, sendo controlado por um operador humano. O lado ucraniano recorreu às soluções comerciais da fabricante chinesa DJI, equipando esses sistemas em fábricas nacionais com granadas capazes de atingir com precisão veículos de combate russos. Em paralelo, o empreendimento ucraniano *Aerorozvidka* passou a produzir drones, com destaque para o R-18. Somado a isso, a Ucrânia tem utilizado veículos aéreos de combate não tripulados *Switchblade* 300 e 600 americanos, bem como o Bayraktar TB2 turco (Westhues 2025). Ademais, a *startup* ucraniana *Swarmer* desenvolveu o AI Copilot que permite que um único operador pilote um enxame de drones, ampliando o poder de combate no nível tático (Onderco 2025).

Por sua vez, os russos empregam os drones KUB-LA (Zysk 2024) e os iranianos Shahed 136, sendo capazes de selecionar e engajar alvos (Weshues 2025). Salienta-se que Moscou realizou testes para aplicação da IA em aeronaves,





como o MIG-35 e o SU-35, incluindo o reconhecimento de alvos e o gerenciamento de informações a bordo (Zysk 2024). Essas novas funcionalidades presentes no domínio aéreo produziram avanços na defesa antiaérea, reduzindo o tempo de reação para essas respostas (Santayana 2024). Simultaneamente foram criadas novas formas de combater essas ameaças, como o Drone F700 desenvolvido pela Fortem. Essa tecnologia encontra-se em fase de testes e visa interceptar e atingir drones russos enviados para atacar as instalações de energia da Ucrânia (Onderco 2025).

O desenvolvimento de sistemas de armas autônomo possibilitou uma perda progressiva do controle humano, como o emprego de tecnologia de enxame de drones em ataques sincronizados (Weshues 2025). Nesse contexto, o dilema entre controle humano e julgamento humano ocorre pelo fato de que alguns sistemas autônomos são extremamente prescritivos na decisão que resulta em engajar um alvo. Portanto, apesar do indivíduo estar envolvido na decisão, atendendo ao critério de controle humano, não fica claro se o julgamento humano está sendo exercido (Onderco 2025).

Ademais, essas tecnologias podem ser aliadas a sistemas de tomada de decisão que possibilitam o emprego de armas sem controle humano (Weshues 2025), como o ecossistema de drones Lancet da Rússia. No modelo de reconhecimento, esse *loitering munition* é capaz de detectar objetos, transmitir sua imagem e realizar ataque, sendo considerado um sistema autônomo. Em paralelo, o Lancet-3 utiliza redes neurais convolucionais para coletar, classificar e analisar as imagens e vídeos obtidos durante o voo, sendo capaz de realizar a tomada de decisão (Santayana 2024). Portanto, a combinação desses sistemas por meio de redes neurais inclui “a capacidade de localizar e destruir um alvo sem orientação humana e retornar ao operador se o alvo não for encontrado” (Zysk 2024, 364). Salienta-se que a retirada do fator humano cria uma “lacuna de responsabilização”, pois a eliminação de uma vida humana por meio de uma tecnologia é vista à luz do Direito Internacional Humanitário como antiético e imoral (Wyatt 2024).

Desse modo, o conflito entre Rússia e Ucrânia demonstra que a inteligência artificial reconfigura a névoa da guerra, transformando a incerteza clausewitziana em novas formas de fricção. A quantidade massiva de dados sobre o alvo e a automação das decisões reduz a imprevisibilidade, ao mesmo tempo em que cria vulnerabilidades inéditas, como falhas algorítmicas, dependência tecnológica e riscos éticos. Assim, a névoa da guerra se reconfigura, migrando parcialmente do campo físico para contornos digitais e cognitivos.





5 Conclusão

A IA aumenta a complexidade do nevoeiro da guerra, conforme observado no conflito da Rússia e Ucrânia. Essa tecnologia quando incorporada a doutrina militar cria diversas vantagens nos diferentes níveis decisórios, como o aumento da eficácia por meio de sistemas autônomos e a redução do ciclo decisório na tomada de decisão, sendo necessário equilibrar a eficiência tecnológica com o julgamento humano. Entretanto, verifica-se que conforme as capacidades militares ofensivas e defensivas da IA foram evoluindo na guerra, os países em disputa organizaram respostas mais precisas e potentes. Esse fato ratifica que a fricção e a automação no combate tornam os conflitos mais incertos e menos decisivos, portanto, não há dissonância entre esses elementos.

Outrossim, verifica-se que os sistemas autônomos que possuem a capacidade de tomada de decisão assistida interferem na natureza subjetiva da guerra, pois um adversário que aceita não possuir controle humano em seus armamentos desequilibra a disputa com oponentes que necessitam de julgamento humano no seu ciclo decisório. Apesar dos problemas vinculados à responsabilização, tanto na esfera ética como jurídica, visualiza-se pouco provável que essas soluções sejam totalmente banidas dos campos de batalha contemporâneos.

Além disso, a principal novidade da guerra entre Rússia e Ucrânia tem sido o emprego em larga escala das soluções baseadas em IA. Nesse sentido, o conflito serve como um campo de provas para acelerar o desenvolvimento de novas tecnologias capazes de impactar a arte militar nos próximos anos. Contudo, os limites e as ambiguidades dessa guerra mediada por dados e algoritmos também estão presentes. Um exemplo é a dependência de sistemas centralizados que geram novas vulnerabilidades a ataques cibernéticos, como o Delta, ocasionando formas inéditas de fricção. Além disso, a transparência do campo de batalha não eliminou a incerteza, mas a deslocou para a confiabilidade dos algoritmos e a integridade dos dados. Outro aspecto se refere à eficácia de muitas dessas tecnologias que dependem criticamente da colaboração com o setor privado e aliados internacionais, resultando na redução da autonomia estratégica dos Estados.

Do exposto, os conflitos contemporâneos se assemelham a laboratórios que envolvem teste de diferentes empresas oriundas de diversos países e de distintos setores. Isso tem possibilitado o desenvolvimento de sistemas dual que aplicam suas soluções no combate real, obtendo *feedback* imediato e incentivo constante para a inovação de seus produtos. Isso possibilita um avanço sem





precedentes para os componentes que envolvem Ciência e Tecnologia, sendo um fator crítico de sucesso em detrimento da modelagem baseada em testes nos ambientes simulados. Ademais, nota-se que o setor civil tem implementado diversas funcionalidades da IA com aplicações militares, demonstrando que pode haver uma tendência de aumento na dependência dessas funcionalidades civis no setor de defesa.

Apesar dos avanços tecnológicos, infere-se que a utilização de sistemas autônomos não impedirá a perda de vidas humanas durante os conflitos armados, possibilitando que adversários assimétricos se utilizem do sofrimento humano e do prolongamento do combate para atingir vitórias decisivas por meio do desgaste do esforço de guerra e da vontade de lutar dos países com maior capacidade militar. Diante disso, as habilidades dos tomadores de decisão precisam ser aprimoradas para fazer frente às tecnologias inovadoras, reduzindo a neblina da guerra.

Referências

- Bellanova, Rocco. 2021. *Digital Surveillance and Security Governance: A Sociotechnical Approach*. Routledge.
- Boyd, John. 2007. *Patterns of conflict*. Defense and the National Interest.
- Bousquet, Antoine. 2009. *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*. Columbia University Press.
- Brose, Christian. 2020. *The Kill Chain: Defending America in the Future of High-Tech Warfare*. Hachette Books.
- Buolamwini, Joy e Timnit Gebru. 2018. “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification”. *Proceedings of Machine Learning Research* 81 (1): 1–15.
- Clausewitz, Carl Von. 2010. *Da Guerra*. Martins Fontes.
- Creveld, Martin V. 1985. *Command in War*. Harvard University Press.
- Daniels, Owen. 2021. *Speeding Up the OODA Loop with AI*. Joint Air Power Competence Centre (JAPCC).
- Elish, Madeleine Clare. 2016. “Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction”. *Engaging Science, Technology, and Society*, 5: 40-60.
- Freedman, Lawrence. 2013. *Strategy: A History*. London, UK: Oxford University Press.
- Galison, Peter. 1994. “Trading Zone: Coordinating Action and Belief.” Em *The Disunity of Science: Boundaries, Contexts, and Power*, organizado por Peter Galison e David Stump. Stanford University Press.





- Goncharuk, Vitaliy. 2024. "Survival of the Smartest? Defense AI in Ukraine". Em *The Very Long Game*, organizado por Heiko Borchert, Torben Schütz e Joseph Verbovsky. Springer Nature.
- Gray, Colin S. 1999. *Modern Strategy*. Oxford University Press.
- Harknett, Richard e Max Smeets. 2020. "Cyber Campaigns and Strategic Outcomes". *Journal of Strategic Studies* 45 (4) 534-567.
- Horowitz, Michael C. 2019. "When Speed Kills: Lethal Autonomous Weapon Systems, Deterrence and Stability". *Journal of Strategic Studies* 42 (6): 764-88.
- Husain, Amir. 2017. *The Sentient Machine: The Coming Age of Artificial Intelligence*. Scribner.
- Johnson, James. 2022. "Automating the OODA Loop in the Age of Intelligent Machines: Reaffirming the Role of Humans in Command-and-Control Decision-Making in the Digital Age". *Defence Studies* 23 (1): 43-67.
- Kania, Elsa B. 2019. *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*. Center for Security and Emerging Technology (CSET).
- Kott, Alexander e Igor Linkov. 2019. *Cyber Resilience of Systems and Networks*. Springer Nature.
- Latour, Bruno. 1991. *We Have Never Been Modern*. Harvard University Press.
- Lindsay, Jon R. 2023. "War Is from Mars, AI Is from Venus: Rediscovering the Institutional Context of Military Automation". *Texas National Security Review* 7 (1): 29-47.
- Lopes, João Ricardo. 2021. "Controle Reflexivo Russo: Teoria Militar e Aplicações". *Coleção Meira Mattos* 15(1) 15-41.
- McMaster, Herbert R. 2009. "The Human Element: When Gadgetry Becomes Strategy". *World Affairs* 171 (3): 31-43.
- Murray, Williamson. 1997. "Clausewitz Out, Computer In: Military Culture and Technological Hubris". Em *War, Strategy and Military Effectiveness*, organizado por Williamson Murray. Cambridge University Press.
- Murray, Williamson and MacGregor Knox. 2022. *A Evolução da Arte da Guerra: das Guerras Medievais aos Ataques Relâmpagos*. Bibliex.
- Onderco, Michal. 2025. Navigating the AI Frontier: Insights from the Ukraine Conflict for NATO's Governance Role in Military AI. *Journal of Strategic Studies*, 1-25.
- Parasuraman, Raja e Victor Riley. 1997. "Humans and Automation: Use, Misuse, Disuse, Abuse". *Human Factors* 39 (2): 230-253.
- Paret, Peter; Michael Howard e Bernard Brodie. 1984. "Ensaios introdutórios". Em *Da Guerra* de Carl Von Clausewitz. Oxford University Press.
- Russell, Stuart e Peter Norvig. 2016. *Artificial Intelligence: A Modern Approach*. Pearson.
- Santayana, José. 2024. "La Inteligencia Artificial y la Guerra de Ucrania". *Cuadernos de Estrategia* 1 (226): 87-104.





- Scharre, Paul. 2018. *Army of None: Autonomous Weapons and the Future of War*. W. W. Norton & Company.
- Scharre, Paul. 2024. *Four Battlegrounds: Power in the Age of Artificial Intelligence*. W. W. Norton & Company.
- Semenenko, Oleh; Oleh Semenko; Nataliia Shynkaruk; Polina Tolok; Serhii Ostrovskiy e Ihor Davydov. 2025. "Forecasts of Transformation in Legal Regulation of Artificial Intelligence for Cybersecurity in Ukraine's Defence Sector". *Interdisciplinary Journal of Applied Science* 9 (14): 1-12.
- Skitka, Linda, Kathleen Mosier e Mark Burdick. 1999. "Automation Bias: Decision Making and Performance in High-Tech Cockpits". *International Journal of Aviation Psychology* 9 (1): 47-63.
- Suchman, Lucy. 2007. *Human-Machine Reconfigurations: Plans and Situated Actions*. Cambridge University Press.
- Westhues, Andreas Heinz. 2025. The Militarization of Artificial Intelligence and the Autonomous Weapons. *Revista UNISCI* 23 (67): 111-136.
- Work, Robert e Greg Grant. 2019. *Beating the Americans at Their Own Game: An Offset Strategy with Chinese Characteristics*. Center for a New American Security (CNAS).
- Wyatt, Austin. 2024. "Lethal Autonomous Weapons Systems and Their Potential Impact on the Future of Warfare." Em *The Routledge Handbook of the Future of Warfare*, organizado por Artur Gruszczak e Sebastian Kaempf. Routledge.
- Zysk, Katarzyna. 2024. "High Hopes Amid Hard Realities: Defense AI in Russia". Em *The Very Long Game*, organizado por Heiko Borchert, Torben Schütz e Joseph Verbovsky. Springer Nature.

