A aeronave de teste de simulação variável em voo X-62A (*Variable In-flight Simulation Test Aircraft,* VISTA) da Lockheed Martin, uma aeronave de treinamento única, é pilotada por um agente de IA, em 13 de fevereiro de 2023, na Edwards Air Force Base, Califórnia (embora os pilotos de segurança estivessem continuamente a bordo). A aeronave voou por mais de 17 horas, e foi a primeira vez que a IA foi acionada em uma aeronave tática. (Foto: Kyle Brasier, Força Aérea dos EUA)

Inteligência artificial na guerra moderna

Inovação estratégica e riscos emergentes

Ryan Atkinson, Ph.D.

Nos últimos anos, a inteligência artificial (IA) conquistou vitórias impressionantes sobre adversários humanos, incluindo o AlphaZero no xadrez, o AlphaGo no Go e o AlphaStar no StarCraft II. A Força Aérea dos Estados Unidos da América (EUA) e a Agência de Projetos de Pesquisa Avançada de Defesa

(Defense Advanced Research Projects Agency, DARPA) criaram o AlphaDogfight para testar a IA contra um piloto humano. A IA enfrentou o piloto vindo diretamente pela frente em um jogo do covarde em alta velocidade, "vencendo de cinco a zero com suas manobras agressivas e precisas que o piloto humano não conseguiu sobrepujar."[1] Esses avanços destacam a crescente habilidade da IA em desafiar e superar as capacidades humanas em cenários complexos, ressaltando seu potencial para transformar ambientes competitivos e estratégicos.

A tomada de decisão se torna cada vez mais automatizada e o envolvimento humano mais reduzido à medida que os sistemas autônomos assumem um controle maior sobre as aeronaves. A Força Aérea dos EUA testou um sistema de IA que pilotou a aeronave tática X-62A, ou VISTA.[2] Esse marco significativo no desenvolvimento de sistemas de IA indica o potencial para futuras operações militares autônomas ou semiautônomas.

As tecnologias de emprego dual estão ganhando cada vez mais importância à medida que as ferramentas de IA evoluem, trazendo riscos e oportunidades emergentes. Essas tecnologias podem ser utilizadas em aplicações civis que servem de base para operações militares, e vice-versa. Por exemplo, as práticas e os precedentes de IA utilizados para direcionar anúncios em mídias sociais para campanhas políticas ou de marketing podem, então, apoiar a comunicação estratégica e as operações psicológicas militares. Novos medicamentos serão desenvolvidos, assim como novas armas químicas, aumentando a necessidade de pesquisas contínuas sobre os riscos e oportunidades correlatos.[3] As tecnologias de emprego dual continuam sendo uma faca de dois gumes nas aplicações de IA.

A inovação em defesa e as parcerias sólidas entre as Forças Armadas e o setor são significativas. Empresas de IA emergentes no setor de defesa oferecem novas iniciativas para inovações entre os aliados. Os casos críticos devem ser encontrados por meio de ênfase na colaboração dentro da ampla rede de titãs do setor de defesa e de novos inovadores emergentes. A IA está mudando rapidamente a tecnologia e as táticas das Forças Armadas, e a natureza de emprego dual dessa tecnologia desafia o desenvolvimento da IA aplicada em ambientes militares.

Ryan Atkinson, Ph.D., é pesquisador de pós-doutorado na Carleton University, em Ottawa, Canadá. Seu trabalho é financiado pela Canadian Defence and Security Network.

Os sistemas autônomos de armas representam um avanço significativo na tecnologia militar, operando sem intervenção humana direta. Aplicações militares benéficas incluem casos específicos do Exército, como sistemas inteligentes de apoio à decisão e reconhecimento de alvo assistido, que podem aliviar a carga mental dos operadores, possibilitando uma tomada de decisão mais rápida.[4] Essa abordagem oferece vantagens, incluindo tempos de resposta rápidos, capacidade de operar em ambientes de alto risco e um risco reduzido para o pessoal humano.

Inteligência generativa e enxames coordenados

As tecnologias emergentes relacionadas a agentes generativos oferecem aplicações de emprego dual. Pesquisadores da Stanford University e da Google demonstraram "agentes de software computacional que simulam um comportamento humano crível", como uma cidade pequena com 25 agentes.[5] Observou-se cooperação no grupo, o que levou a comportamentos sociais emergentes para "trocar informações, formar novos relacionamentos e coordenar atividades conjuntas."[6]

A arquitetura permite que os agentes generativos "lembrem, recuperem, reflitam, interajam com outros agentes e planejem em meio a circunstâncias que evoluem dinamicamente".[7] Os grandes modelos de linguagem são utilizados para "suplementar essas capacidades, apoiando a coerência de agentes a longo prazo, a capacidade de gerenciar uma memória que evolui dinamicamente e a produção recursiva de reflexões de nível mais elevado".[8]

As democracias resilientes precisam, inerentemente, de mecanismos internos adaptáveis para se ajustar às mudanças e lidar rapidamente com situações inesperadas. A aplicação dos modelos de linguagem em cenários do mundo real frequentemente resulta em consequências imprevistas e emergentes. As democracias precisam, de forma proativa, desenvolver contramedidas para enfrentar os riscos emergentes relacionados ao uso generalizado da IA generativa e dos grandes modelos de linguagem, o que acarreta uma camada adicional de desafios de segurança. O abuso malicioso dos modelos de linguagem demonstra um imenso desafio para as eleições e os processos democráticos futuros.[9]

Os riscos relacionados às operações de influência estrangeira que utilizam vídeos e áudios com

A utilização de drones autônomos operados por inteligência artificial em enxames tem grande potencial para causar destruição extensa e em larga escala em alvos designados. As forças visadas teriam imensa dificuldade técnica para se defender de um primeiro ataque em massa e amplamente coordenado contra múltiplos alvos. O emprego simultâneo de um grande número de drones poderia sobrecarregar as capacidades materiais de uma força de defesa, bem como o comando e controle e a governança civil de um defensor em questão de horas, ou até minutos. É relevante destacar que, em junho de 2024, o Exército de Libertação Popular da China conduziu exercícios com drones, incorporando técnicas de enxame, voltados para a tomada de ilhas. Esses exercícios refletiram claramente as ações que provavelmente seriam adotadas em uma invasão de Taiwan. (Foto cedida pelo Exército dos EUA/Shutterstock)

deepfake estão se tornando cada vez mais personalizados e específicos para cada situação. Outras pesquisas devem abordar a proliferação das operações de informação patrocinadas pelo Estado, que utilizam a desinformação gerada para promover "mal-entendidos generalizados, alimentar divisões sociais e afetar negativamente os sistemas econômicos e políticos."[10] A automação também foi empregada no comportamento de grupo envolvendo drones que compartilham informações entre si no enxame, sendo de imenso valor para as operações militares. Pesquisas sobre a inteligência dos enxames envolveram agentes autônomos para aplicações militares, e os testes estão em andamento nos EUA e na China.[11]

Os drones representam um desafio significativo ao armamento convencional. No Mar Vermelho, um drone de USD 2.000 derrubou um míssil de USD 2 milhões.[12] Na Ucrânia, drones de USD 400 estão sendo usados para destruir carros de combate de USD 2 milhões.[13] Esse forte contraste destaca a crescente disparidade entre o custo dos meios militares tradicionais e a acessibilidade e eficácia da tecnologia moderna de drones.

O desenvolvimento da IA da China

Em 2021, o setor de IA da China valia CNY 150 bilhões (USD 23,2 bilhões) e deve chegar a mais de CNY 400 bilhões (USD 55 bilhões) até 2025.[14] O Plano de Desenvolvimento de Inteligência Artificial de Próxima Geração da China estabeleceu uma meta para que a IA contribua com USD 150 bilhões para o PIB chinês até 2030.[15] Em agosto de 2023, Pequim aprovou o lançamento público de tecnologias de IA generativa das empresas chinesas Tencent, Baidu, Huawei Technologies, Alibaba Group, JD.com, ByteDance, iFlytek e Kuaishou Technology.[16]

Em setembro de 2023, a Microsoft divulgou um relatório que demonstrou como as estratégias de IA generativa são usadas em operações de influência conduzidas pela República Popular da China (RPC).[17] O Departamento de Justiça dos EUA denunciou um grupo chamado Grupo de Trabalho do Projeto Especial 912, vinculado ao Ministério de Segurança Pública da China, que operava uma fábrica de *trolls* nas mídias sociais, que "criou milhares de perfis on-line falsos e espalhou propaganda do PCC direcionada aos ativistas pró-democracia."[18]

O relatório da Microsoft observou que, em março de 2023, supostas operações de influência da RPC "nas mídias sociais ocidentais começaram a utilizar a [IA] generativa para criar conteúdo visual", o que "já gerou níveis mais elevados de engajamento de usuários de mídias sociais autênticos."[19] As operações de informação da China se tornarão mais sofisticadas à medida que os aplicativos de IA generativa se tornarem cada vez mais direcionados a alvos específicos.

O relatório mencionou os "estúdios multilíngues de celebridades da Internet" do PCC, com 230 funcionários e afiliados da mídia estatal, que se fazem passar por influenciadores independentes nas mídias sociais, com foco na mídia social ocidental.[20] A Microsoft observou que, em 2022 e 2023, "novos influenciadores continuam a estrear a cada sete semanas, em média".[21] A Rádio Internacional da China é uma das várias entidades que "recrutaram, treinaram, promoveram e financiaram" tais capacidades, juntamente com outras entidades de mídias patrocinadas pelo Estado, para atingir 103 milhões de pessoas em 40 idiomas.[22]

(Foto: Adobe Stock)

Várias plataformas de atividades visadas pela China incluem empresas como Vimeo, Wattpad, Indeed, Rotten Tomatoes, Instagram, Quora, Medium, Facebook, Reddit, Tumblr, YouTube, Twitter/X, Pinterest, Blogger, TikTok, Flickr e LinkedIn.[23] Uma rede de influência patrocinada representa um desafio significativo, pois populações ocidentais podem ser influenciadas por personalidades patrocinadas por governos estrangeiros, possibilitando operações de subversão em aplicativos de compartilhamento de vídeos.

A Microsoft forneceu exemplos de janeiro de 2022 de uma campanha alinhada ao PCC que visava a "organização não governamental espanhola Safeguard Defenders, após esta ter revelado a existência de mais de 50 delegacias de polícia chinesas no exterior".[24] A campanha implantou 1.800 contas em plataformas de mídia social e dezenas de sites para divulgar memes, vídeos e mensagens alinhados ao PCC criticando os EUA e outras democracias. As mensagens eram compartilhadas em holandês, grego, indonésio, sueco, turco, uigur e outros idiomas em plataformas como Fandango, Rotten Tomatoes, Medium, Chess.com e VK.

Redes aliadas de inovação em defesa

Os países buscam superioridade tecnológica em IA para obter vantagens competitivas em vários domínios, incluindo capacidades militares, produtividade econômica e inovação tecnológica. Nos últimos anos, os aliados da Organização do Tratado do Atlântico Norte (OTAN) têm se concentrado significativamente na inovação da defesa e nos desafios correspondentes. A OTAN lançou sua primeira estratégia de IA em outubro de 2021.[25] Uma estratégia de IA revisada foi lançada na Cúpula de Washington em julho de 2024.[26]

O Defense Innovation Accelerator for the North Atlantic, DIANA, (Acelerador de Inovação em Defesa para o Atlântico Norte, em tradução livre) da OTAN, trabalha com governos, indústria e o meio acadêmico no apoio ao desenvolvimento de tecnologias emergentes na América e na Europa. O programa oferece aos inovadores acesso a uma rede profissional para ajudar no desenvolvimento de um programa acelerador personalizado.[27] Além da IA, a OTAN tem se concentrado em várias outras tecnologias emergentes e disruptivas, que incluem sistemas autônomos, tecnologias quânticas, biotecnologia e tecnologias de aperfeiçoamento humano, sistemas hipersônicos, setor espacial, materiais e fabricação inovadores, energia e propulsão, bem como redes de comunicação de próxima geração.[28]

O DIANA entrou em operação em meados de 2023, lançando sua primeira rodada de desafios para promover a

inovação em necessidades de segurança críticas específicas, visando o avanço tecnológico.[29] Em 2023, a OTAN lançou a primeira rodada de desafios para apoiar o desenvolvimento de tecnologias de emprego dual a fim de resolver problemas de resiliência energética, sensoriamento e vigilância e compartilhamento seguro da informação.[30]

O DIANA lançou cinco novos desafios em 2024, que incluem energia e potência, segurança de dados e informação, sensoriamento e vigilância, saúde e desempenho humano e infraestrutura e logística críticas.[31] O compromisso do DIANA é promover soluções de ponta e reforçar as capacidades estratégicas da OTAN em um cenário global cada vez mais complexo. Essas iniciativas se alinham à necessidade crítica de inovações robustas em defesa e colaborações estratégicas essenciais para combater as aplicações militares da IA em rápida evolução. ■

Referências

1. "AlphaDogfight Trials Foreshadow Future of Human-Machine Symbiosis", Defense Advanced Research Projects Agency (DARPA), 26 August 2020, https://www.darpa.mil/news-events/2020-08-26.

2. "ACE Program's AI Agents Transition from Simulation to Live Flight", DARPA, 13 February 2023, https://www.darpa.mil/news-events/2023-02-13.

3. Fabio Urbina et al., "AI in Drug Discovery: A Wake-up Call", *Drug Discovery Today* 28, no. 1 (January 2023): Article 103410, https://doi.org/10.1016/j.drudis.2022.103410.

4. David Oniani et al., "Adopting and Expanding Ethical Principles for Generative Artificial Intelligence from Military to Healthcare", *npj Digital Medicine* 6, no. 1 (2 December 2023): p. 1-10, https://doi.org/10.1038/s41746-023-00965-x.

5. Joon Sung Park et al., "Generative Agents: Interactive Simulacra of Human Behavior", arXiv, 5 August 2023, http://arxiv.org/abs/2304.03442.

6. Ibid., sec. 3.4.

7. Ibid., sec. 1.

8. Ibid.

9. Tom Di Fonzo, "What You Need to Know About Generative AI's Emerging Role in Political Campaigns", Tech Policy Press, 12 October 2023, https://www.techpolicy.press/what-you-need-to-know-about-generative-ais-emerging-role-in-political-campaigns/.

10. U.S. Department of Homeland Security, *Unveiling the Dark Art: Investigating the Nexus between Generative Artificial Intelligence and Foreign Malign Influence* (Washington, DC: U.S. Department of Homeland Security, 29 September 2023), https://www.dhs.gov/sites/default/files/2023-09/23_0906_oia_GAI_ForeignMalignInfluence_508.pdf.

11. Matt Berg, "Killer Robot Swarms, an Update", Politico, 4 January 2024, https://www.politico.com/newsletters/digital-future-daily/2023/02/07/killer-robot-swarms-an-update-00081623.

12. Laura Seligman e Matt Berg, "A $2M Missile vs. a $2,000 Drone: Pentagon Worried over Cost of Houthi Attacks", Politico, última atualização em 20 dez. 2023, https://www.politico.com/news/2023/12/19/missile-drone-pentagon-houthi-attacks-iran-00132480.

13. Veronika Melkozerova, "The Future of Warfare: A $400 Drone Killing a $2M Tank", Politico, 26 October 2023, https://www.politico.eu/article/future-warfare-400-army-strike-drone-unit-2m-tank/.

14. Iris Deng, "Shenzhen Is First Chinese City to Draft Regulations Specifically for AI", South China Morning Post (site), 30 June 2021, https://www.scmp.com/tech/policy/article/3139319/shenzhen-chinas-silicon-valley-plans-turbocharge-local-ai-development.

15. Eamon Barrett, "AI in China: TikTok Is Just the Beginning", *Fortune* (site), 20 January 2020, https://fortune.com/longform/tiktok-app-artificial-intelligence-addictive-bytedance-china/.

16. Zhou Xin, "Too Late Now for US to Hold Back China in Global AI Race", Nikkei Asia, 24 October 2023, https://asia.nikkei.com/Opinion/Too-late-now-for-U.S.-to-hold-back-China-in-global-AI-race.

17. Microsoft Threat Intelligence, "Sophistication, Scope, and Scale: Digital Threats from East Asia Increase in Breadth and Effectiveness" (Redmond, VA: Microsoft, September 2023), p. 6, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW.

18. Ibid., p. 6.

19. Ibid.

20. Ibid., p. 7.

21. Ibid.

22. Ibid.

23. Ibid., p. 10.

24. Ibid.

25. "Summary of the NATO Artificial Intelligence Strategy", NATO, 22 October 2021, https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

26. "NATO Releases Revised AI Strategy", NATO, 10 July 2024, https://www.nato.int/cps/en/natohq/news_227234.htm.

27. "NATO DIANA Announces First Cohort of Innovators, Launches Call for Mentors", NATO, 4 December 2023, https://www.nato.int/cps/en/natohq/news_220930.htm.

28. "Emerging and Disruptive Technologies", NATO, 22 June 2023, https://www.nato.int/cps/en/natohq/topics_184303.htm.

29. "Defense Innovation Accelerator for the North Atlantic", NATO, 5 July 2024, https://www.nato.int/cps/en/natohq/topics_216199.htm.

30. "NATO's Innovation Accelerator Becomes Operational and Launches First Challenges", NATO, 19 June 2023, https://www.nato.int/cps/en/natohq/news_215792.htm.

31. "2024 DIANA Challenge Programme Call for Proposals", NATO, acesso em 22 jul. 2024, https://www.diana.nato.int/resources/site1/general/2024_challenge_programme_web.pdf.