The Lockheed Martin Variable In-flight Simulation Test Aircraft X-62A (VISTA), a one-of-a-kind training aircraft, is piloted by an AI agent on 13 February 2023 at Edwards Air Force Base, California (although safety pilots were continuously on board). The aircraft flew for more than seventeen hours and was the first time AI engaged on a tactical aircraft. (Photo by Kyle Brasier, U.S. Air Force)

Artificial Intelligence in Modern Warfare

Strategic Innovation and Emerging Risks

Ryan Atkinson, PhD

In recent years, artificial intelligence (AI) has achieved notable victories over human opponents, including AlphaZero in Chess, AlphaGo in Go, and AlphaStar in StarCraft II. The United States Air Force and the Defense Advanced Research Projects Agency (DARPA) have created AlphaDogfight to test AI against a human pilot. The AI came at the pilot from the front in a speeding-precise game of chicken, "winning 5-0 through aggressive and precise maneuvers the human pilot couldn't outmatch."[1] These advancements highlight AI's growing capability to challenge and surpass human skills in complex scenarios, underscoring its potential to reshape competitive and strategic environments.

Increasingly, decision-making is automated and human involvement is lessened as autonomous systems have more control over aircraft. The U.S. Air Force tested an AI system that piloted the X-62A or VISTA tactical aircraft.[2] This significant milestone in developing AI systems indicates the potential for future autonomous or semi-autonomous military operations.

Dual-use technologies are becoming increasingly significant as AI tools evolve, presenting emerging risks and opportunities. These technologies can be applied to civilian uses that inform military operations and vice versa. For instance, precedents and practices of AI used to target advertisements on social media for marketing or political campaigns can then support military strategic communication and psychological operations. New medicines will be developed, but so will new chemical weapons, furthering the need for ongoing research into related risks and opportunities.[3] Dual-use technologies remain a double-edged sword of AI applications.

Defense innovation and strong partnerships between the military and industry are significant. Emerging AI firms within the defense industry provide new initiatives for innovations among allies. Critical cases are to be found through an emphasis on collaboration within the extensive network of defense industry titans and new emerging innovators. AI is quickly changing military technology and tactics, and the dual-use nature of the technology challenges the development of applied AI in military settings.

Ryan Atkinson, PhD, is a postdoctoral Fellow at Carleton University, Ottawa, Canada. His work is funded by the Canadian Defence and Security Network.

Autonomous weapon systems represent a significant advancement in military technology, operating without direct human intervention. Beneficial military applications include Army-specific cases such as intelligent decision-support systems and aided target recognition, which can reduce the mental load for operators, enabling faster decision-making.[4] This approach provides advantages, including rapid response times, the ability to operate in high-risk environments, and a reduced risk to human personnel.

Generative Intelligence and Coordinated Swarms

Emerging technologies related to generative agents provide dual-use applications. Researchers at Stanford and Google demonstrated "computational software agents that simulate believable human behavior," resembling a small town of twenty-five agents.[5] Cooperation was observed among the group, which led to emergent social behaviors to "exchange information, form new relationships, and coordinate joint activities."[6]

The architecture allows generative agents to "remember, retrieve, reflect, interact with other agents, and plan through dynamically evolving circumstances."[7] Large language models are used to "supplement those capabilities to support longer-term agent coherence, the ability to manage dynamically evolving memory, and recursively produce higher-level reflections."[8]

Resilient democracies inherently need adaptable internal mechanisms to adjust to change and address unexpected situations swiftly. Applying language models to real-world scenarios often lead to unforeseen and emergent consequences. Democracies must proactively create countermeasures to address the emerging risks associated with the widespread use of generative AI and large language models, which add an additional layer of security challenges. The malicious abuse of language models demonstrates an immense challenge for future elections and democratic processes.[9]

The risks associated with foreign influence operations using deep faked video and audio are increasingly tailored and case specific. Further research must address the proliferation of state-sponsored information operations using generated disinformation to foster "widespread misunderstanding, foment social divisions, and negatively impact economic and political systems."[10] Automation has also been applied to group behavior

involving drones sending information to others in the swam, providing immense value for military operations. Research into swarm intelligence has involved autonomous agents for military applications, and testing is currently ongoing in the United States and China.[11]

Drones have posed a significant challenge to conventional weaponry. In the Red Sea, a $2,000 drone took down a $2 million missile.[12] In Ukraine, $400 drones are being employed to destroy $2 million tanks.[13] This stark contrast underscores the widening gap between the cost of traditional military assets and the affordability and effectiveness of modern drone technology.

The use of artificial intelligence autonomous drones employed in swarms has significant potential to inflict broad, large-scale destruction on designated targets. Targeted forces would have immense technical difficulty in defending themselves against a massive, broadly coordinated first strike against multiple targets. The simultaneous employment of large numbers of drones could overwhelm the material capabilities of a defending force as well as a defender's command and control and civil governance within a matter of hours, if not minutes. Of note, in June 2024, China's People's Liberation Army conducted drone exercises, including swarm techniques, focused on island seizure that transparently mirrored actions that it would likely take in an invasion of Taiwan. (Photo courtesy of the U.S. Army/Shutterstock)

China's AI Build-up

As of 2021, China's AI industry was worth 150 billion yuan (US$23.2 billion) and is expected to reach more than 400 billion yuan (US$55 billion) by 2025.[14] China's Next Generation AI Development Plan set a target for AI to contribute US$150 billion to China's GDP by 2030.[15] In August 2023, Beijing approved the public release of generative AI technologies from Chinese firms Tencent, Baidu, Huawei Technologies, Alibaba Group, JD.com, ByteDance, iFlytek, and Kuaishou Technology.[16]

Microsoft released a report in September 2023 that demonstrated how generative AI strategies are used in influence operations conducted by the People's Republic of China (PRC).[17] The U.S. Department of Justice reported a group called 912 Special Working Group within China's Ministry of Public Security that operated a troll farm on social media, which "created thousands of fake online personas and pushed CCP propaganda targeting pro-democracy activists."[18]

The Microsoft report noted that in March 2023, suspected PRC influence operations "on Western social media have begun to leverage generative [AI] to create visual content," which "has already drawn higher levels of engagement from authentic social media users."[19] China's information operations will only get more sophisticated, as applications of generative AI become increasingly tailored to specific targets.

The report described the CCP's "multilingual internet celebrity studios," staffed by 230 state media employees and affiliates posing as independent social media influencers, aimed at Western social media.[20] Microsoft noted that in 2022 and 2023, "new influencers continue to debut every seven weeks on average."[21] China Radio International is one of the numerous entities that "recruited, trained, promoted, and funded" such capabilities among other state-sponsored media entities to reach 103 million people in forty languages.[22]

Various platforms of targeted activity by China include firms such as Vimeo, Wattpad, Indeed, Rotten Tomatoes, Instagram, Quora, Medium, Facebook, Reddit, Tumblr, YouTube, Twitter/X, Pinterest, Blogger, TikTok, Flickr, and LinkedIn.[23] A sponsored network of influence demonstrates a significant challenge where Western populations can be influenced by personalities sponsored by foreign governments, providing the possibility for subversion operations over video-sharing apps.

Microsoft provided examples from January 2022 of a CCP-aligned campaign which targeted "Spanish non-governmental organization Safeguard Defenders after it exposed the existence of more than 50 overseas Chinese police stations."[24] The campaign deployed 1,800 accounts across social media platforms and

(Photo by Adobe Stock)

dozens of websites to spread CCP-aligned memes, videos, and messages criticizing the U.S. and other democracies. The messages were shared in Dutch, Greek, Indonesian, Swedish, Turkish, Uyghur, and more on platforms like Fandango, Rotten Tomatoes, Medium, Chess.com, and VK.

Allied Networks of Defense Innovation

Countries pursue technological superiority in AI to gain competitive advantages in various domains, including military capabilities, economic productivity, and technological innovation. In recent years, NATO allies have been focused significantly on defense innovation and related challenges. NATO released its first-ever AI strategy in October 2021.[25] A revised AI strategy was released at the Washington Summit in July 2024.[26]

NATO's Defense Innovation Accelerator for the North Atlantic (DIANA) works with governments, industry, and academia to support the development of emerging technologies in America and Europe. The program provides innovators access to a professional network to help develop a customized accelerator program.[27] Beyond AI, NATO has focused on numerous other emerging disruptive technologies, which include autonomous systems, quantum technologies, biotechnology and human enhancement technologies, hypersonic systems, space, novel materials and manufacturing, energy and propulsion, and next-generation communications networks.[28]

DIANA became operational in the summer of 2023, where it launched its first round of challenges to foster innovation on specific critical security needs to target technological advancement.[29] In 2023, NATO launched the first round of challenges to support the development of dual-use technologies to solve problems on energy resilience, sensing and surveillance, and secure information sharing. [30]

DIANA launched five new challenges in 2024, which include energy and power, data and information security, sensing and surveillance, human health and performance, and critical infrastructure and logistics.[31] DIANA is committed to fostering cutting-edge solutions and bolstering NATO's strategic capabilities in an increasingly complex global landscape. These initiatives align with the critical need for robust defense innovations and strategic collaborations essential to counter AI's rapidly evolving military applications. ■

Notes

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): 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 and Matt Berg, "A $2M Missile vs. a $2,000 Drone: Pentagon Worried over Cost of Houthi Attacks," Politico, last updated 20 December 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* (website), 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* (website), 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), 6, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW.

18. Ibid., 6.

19. Ibid.

20. Ibid., 7.

21. Ibid.

22. Ibid.

23. Ibid., 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, accessed 22 July 2024, https://www.diana.nato.int/resources/site1/general/2024_challenge_programme_web.pdf.