MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

NATO's AI Push and Military Implications

Sanur Sharma

May 24, 2022

Summary

NATO countries are adopting Emerging and Disruptive Technologies (EDTs) to maintain their strategic advantage and to mitigate transnational threats. Russia's offensive cyber hostilities and China using Artificial Intelligence (AI) for augmenting its high-tech warfare mechanisms have emerged as the contributing factors for NATO to upscale its technological efforts in this field. The rise in use of autonomous systems in military applications is changing the face of the battlefield by enabling new forms of military functions, over and above the conventional systems, thus enabling the execution of higher coercive actions. Going forward, NATO will have to deal with issues related to governance, autonomy, and overcoming the vulnerabilities associated with AI-enabled weapon systems.

Introduction

The technological advancements in Artificial Intelligence (AI), machine learning, big data analytics, robotics, quantum computing and virtual reality have led to the rise in use of autonomous systems in military applications. This is changing the face of the battlefield by enabling new forms of military functions, over and above the conventional systems, thus enabling the execution of higher coercive actions. The North Atlantic Treaty Organization (NATO) countries are also adopting such emerging technologies to maintain their strategic advantage and to mitigate transnational threats.

Russia's offensive cyber hostilities and China's military adoption of AI for augmenting its high-tech warfare mechanisms have emerged as the contributing factors for NATO to upscale its technological efforts in Emerging and Disruptive Technologies (EDTs). NATO is making ambitious investments in EDTs to ensure interoperability and standardisation among member states.

This Issue Brief takes stock of the current strategic surge by NATO in AI adoption and its ongoing efforts to exploit EDTs for defence innovation and adoption. It discusses the role of AI in contemporary conflicts, specifically NATO's response to the Russia–Ukraine conflict, and explores the vulnerabilities in the AI systems as well as the challenges and limitations in AI adoption by NATO.

NATO's Technological Push

The US National Security Commission Report of 2021 states that China is leapfrogging to new technologies by investing in intelligentised warfare like swarm drones and using AI for reconnaissance, electromagnetic countermeasures and coordinated firepower strikes.[1] The US is jointly working with its allies on the policy implications of such new technology. It is also partnering with countries like Canada, Denmark, Estonia, the UK, France and Norway, to work on military standards on AI.[2]

In October 2021, NATO formally adopted the first AI strategy on the responsible military use of AI with three core tasks: collective defence, crisis management and cooperative security.[3] NATO's strategy aims to accelerate the uptake of AI for military

[1] **"The Final Report-2021"**, National Security Commission on Artificial Intelligence, USA, 5 May 2022.

[2] Helen Warrell, **"NATO Allies Need to Speed Up AI Defence Co-operation"**, *Financial Times*, 8 June 2021.

[3] Zoe Stanley-Lockman and Edward Hunter Christie, **"An Artificial Intelligence Strategy for NATO"**, *NATO Review*, 25 October 2021.

systems.[4] The six principles of the NATO's AI strategy include: Lawfulness, Responsibility and Accountability, Explainability and Traceability, Reliability, Governability and Bias Mitigation.[5] This strategy aims to protect, monitor and innovate AI and related disruptive technologies in a phased manner to establish political support for AI military projects.

The strategic surge in EDTs is driven by the accelerated investment towards the military adoption and innovation of EDTs and maintaining a sustainable innovation ecosystem that can be achieved through civil–military collaboration. In 2021, NATO endorsed the strategy on EDTs that included AI and machine learning among the seven identified key technologies (Data, AI, Autonomy, Quantum, Space, Biotechnology, and Hypersonic).[6] The strategy plans to invest US$ 1 billion in building test centres across Europe and North America, focusing on emerging technologies like AI, Quantum and hypersonics.[7]

In the NATO Summit held at Brussels in 2021, as a part of the NATO 2030 Agenda, NATO's new Defence Innovation Accelerator for the North Atlantic (DIANA) was launched. It aims to maintain NATO's technological edge compared to nations like China and Russia, which are challenging the West with their accelerated investments to build technological capacity and use offensive subversive measures.

DIANA has been assigned to manage the NATO Innovation Fund, receiving a funding of US$ 82.6 million a year for 15 years.[8] It will explore the future roadmap of implementation of advanced technologies and competition to foster transatlantic cooperation.[9] At present, there are 10 accelerator sites with more than 50 test centres in technological hubs across the states.[10] The NATO advisory group on EDTs is an external body that advises NATO on the optimisation of its innovation efforts. This group provides recommendations on improving collaboration and partnerships with the private sector, industry, and academia. In addition, there are other bodies like the NATO Advisory board, Allied Command Transformation (ACT), NATO's Science and Technology Organisation (STO), and NATO Communication and Information Agency (NCIA) that support the alliance's adoption of deep technologies and EDTs.

---

[4] Peter Burt, **"NATO's New AI Strategy: Lacking in Substance and Lacking in Leadership"**, *NATO WATCH*, 8 November 2021.

[5] **"Summary of the NATO Artificial Intelligence Strategy"**, North Atlantic Treaty Organization, 22 October 2021.

[6] **"Emerging and Disruptive Technologies"**, North Atlantic Treaty Organization, 7 April 2022; **"Science & Technology Trends 2020-2040"**, NATO Science & Technology Organization, March 2020.

[7] Ben Wodecki, **"NATO at Risk of Losing AI Innovation Race to Russia, China"**, *AI Business*, 5 April 2022.

[8] Ibid.

[9] Simona R. Soare, **"Innovation as Adaptation: NATO and Emerging Technologies"**, The German Marshall Fund of the United States (GMF), 11 June 2021.

[10] "Emerging and Disruptive Technologies", No. 6.

NATO's AI Influence in Russia–Ukraine Confrontations

AI has been a contributing agent in weaponising cyberspace and augmenting cyberwarfare to the next level in modern battlefield scenarios. While some of its uses such as in scaling of data analytics, data fusion, deep fakes, cyber defence have matured, its use in autonomous weapon systems and other complex operational applications are at a nascent stage.

AI has been aggressively used to spread disinformation in the Russia–Ukraine War. Machine learning algorithms have been used to amplify misleading and fake content on social media platforms, like doctored videos of invading forces and fake live streams. On the other hand, it has also been used for anomaly detection, identification of disinformation and for cybersecurity. AI uses natural language processing algorithms, machine learning and deep learning to identify anomalies in the text data, images and videos.

Russia is said to have used AI-enabled systems not only on the battlefield but also in cyberspace, targeting the critical infrastructures of Ukraine.[11] Russian troll farms have been alleged to have used AI-enabled systems to generate human faces for fake propagandist personas on social media platforms like Twitter, Instagram and Facebook.[12] NATO countries have also used AI to help Ukraine counter such AI-based attacks. Private companies are also playing a role in the unfolding AI battlespace. US-based companies like Snorkel AI, a data science platform, has made its services accessible to federal authorities for the detection of anomalous signals and adversary communications in order to access high-value information for better decision-making.[13]

Similarly, Ukraine has been given free access to Clearview AI facial recognition software, which has a database of 2 billion photos crawled from Russian social media platforms. This software is being used for the detection of Russian forces and to identify the dead and gauge the spread of disinformation in cyberspace.[14] AI's analytical potential has been tapped by companies even before the Russia–Ukraine war started. In December 2021, a geospatial data firm, SpaceKnow, claimed to have detected a military presence in Yelna, a Russian town.

The Russia–Ukraine conflict has become a test case for AI adoption in modern warfare. The US is using the conflict as a test-bed for many of its AI projects with the

[11] Patrick Howell O'Neill, **"How a Russian Cyberwar in Ukraine could Ripple Out Globally"**, *MIT Technology Review*, 21 January 2022; Tom Burt, **"Disrupting Cyberattacks Targeting Ukraine"**, Microsoft, 7 April 2022.

[12] Kyle Wiggers, **"AI Weekly: The Russia-Ukraine Conflict is a Test Case for AI in Warfare"**, *Venture Beat*, 4 March 2022.

[13] Ibid.

[14] Paresh Dave and Jeffrey Dastin, **"Ukraine has Started Using Clearview AI's Facial Recognition during War"**, *Reuters*, 15 March 2022.

Pentagon's 'Maven' project having contributed to the detection and classification of objects of interest from various drone footage through AI and Machine Learning (ML) algorithms. It has been reported that the Pentagon has been using AI and ML tools to collect a vast amount of data on the Russia–Ukraine war and analyse it to learn and generate battlefield intelligence about the Russian command and control strategies.[15]

The advanced AI-enabled systems with the US Department of Defense (DoD) are said to have been used for overseeing the battlefield and collecting and archiving signals intelligence. It was stated at the Defense One's Genius AI Summit in April 2022 that all this information will be fed into systems for training of machine learning algorithms to support future decision-making processes.[16] It is believed that the US and NATO allies have already built such AI-enabled cyber weapons and defences, information about which is said to be highly classified.[17]

The US DoD and its allies have taken advantage of these advanced tools to gather critical information from the publically available image data to thwart Russian attacks in Ukraine. This war data will also help NATO allies anticipate adversary attacks, their behaviour, and the use of advanced technologies in the real world by countries like China and Russia. This intelligence will also augment multifactor analysis and modelling changes dynamically by integrating different technological platforms.

Due to the sanctions imposed on Russia as a result of the Russia–Ukraine war, its AI development is expected to slow down. The ongoing conflict highlights the constraints around the use of AI. Despite AI-enabled cyber-attacks and misinformation campaign by Russia, Ukraine has mounted effective counter-cyber operations.[18] Russia's limited use of AI in the conflict can be explained through the existing vulnerabilities in the AI systems that can be exploited in many ways. One hypothesis for Russia's limited use of AI could be the trust in such systems where it is a matter of lives and military objectives at stake.[19]

The vulnerabilities in the AI systems can include data poisoning and input attacks, attacking the supply pipelines by simply crafting data and feeding it to public

[15] Patrick Tucker, **"AI is Already Learning from Russia's War in Ukraine, DOD Says"**, Defense One, 21 April 2022.

[16] Ibid.

[17] Branka Marijan, **"Beyond Ukraine: AI and the Next US-Russia Confrontation"**, Centre for International Governance Innovation (CIGI), 14 February 2022.

[18] Eric Tegler, **"The Vulnerability of AI Systems May Explain Why Russia Isn't Using Them Extensively in Ukraine"**, Forbes, 16 March 2022.

[19] Ibid.

resources, white-box and black-box attacks.[20] There is always a chance of orchestrated and conflicting data in the face of AI models to derail them and to exploit the vulnerabilities in the algorithms, and active manipulation by the adversaries can be induced.

Defense Advanced Research Projects Agency (DARPA) has launched a Guaranteeing AI Robustness against Deception (GARD) programme. Under this programme, development efforts are being made to establish a theoretical foundation for defensible ML and the creation and testing of such systems.[21] The Army Research Laboratory (ARL) is working with the Internet of Battlefield Things Collaborative Research Alliance (IoBT-CRA) to explore the use of ML and intelligent technology on the battlefield and strengthen the collaboration between autonomous actors and human soldiers in combat. They are also working on methods to understand the challenges of AI-enabled systems employed on the battlefield and to make them less susceptible to attacks.[22]

AI technology in modern warfare will be an intractable weapon in future conflicts beyond Ukraine. Countries trying to achieve a technological edge over others have started considerable investments in AI technology to strengthen their militaries. NATO has invested US$ 1 billion to develop new AI defence technologies. The US DoD has also planned to invest US$ 874 million in AI-related technologies as a part of their army research and development budget (federal fiscal year 2022 DoD budget).[23] The UK DoD is funding suppliers to work with Defence Science & Technology Lab (Dstl) on AI projects which were £7million for the year 2021/22 and is supposed to increase to £29 million in the next year.[24]

NATO's AI Adoption: Challenges and Limitations

The influence of AI on NATO comes with a set of opportunities, challenges and risks. Its adoption process has been incremental and prescriptive. The rising geopolitical conflicts and the use of AI in such conflicts have required the establishment of a dynamic ecosystem to support interoperability. The military adoption of AI requires an innovation ecosystem that is self-sufficient, supports deterrence and resilience, and encompasses the strategic innovation process.

---

[20] Marcus Comiter, **"Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It"**, Belfer Center for Science and International Affairs, Harvard Kennedy School, August 2019.

[21] Eric Tegler, No. 18.

[22] **"Internet of Battle Things (IoBT) Collaborative Research Alliance (CRA)"**, Military History Fandom, 15 May 2022.

[23] Kyle Wiggers, No. 12.

[24] Norbert Neumann, **"Defence Faces AI Strategy Implementation Challenges"**, Army Technology, 7 January 2022.

NATO's AI strategy raises many concerns related to the AI-driven autonomous weapon systems, as it does not adequately address the development of such systems, its deployment and governance. The AI strategy mostly talks about the ethical and responsible use of AI and has omitted the challenges related to the use of lethal autonomous weapon systems. For the US, its priorities lie in ensuring responsible use of AI-enabled systems with their allies for operational and data sharing. It remains to be seen if all the 30 NATO states agree on the same rules and would be willing to agree on practical guidelines for the operational use of AI-enabled systems.

Another challenge for NATO is to standardise rules for all member states in dealing with AI-enabled autonomous weapon systems. Countries like Turkey are working on autonomous weapons and have developed AI-enabled loitering munitions. Turkey has requested the US for upgraded F-16 fighter jets that are said to be AI-enabled.[25] The Biden Administration has asked the Congress to approve the upgrade of Turkey's F-16 fighter jet fleet.[26] Turkey's armed drones have also been used in the Ukraine conflict. For smooth functioning of such systems, it will be necessary for all NATO members to have standardised rules when it comes to deployment of such systems.

Also, there is no transparent allocation of roles for different NATO bodies, and "no dedicated line of funding" for its AI strategy.[27] The finances are shared through multiple funding like NATO Innovation Fund and DIANA which manages funding for various other projects leading to uncertainty over availability of funds and budget cuts. This will be a significant challenge for the effective implementation of the AI strategy.[28] Some other challenges with the adoption of AI strategy through innovation include fragmented national innovation initiatives, allied technological categorisation and digitisation gaps, speed of adoption and spending levels and the underuse of NATO's mechanisms to undertake collaborative defence innovation.[29]

NATO will also have to focus on the vulnerabilities and intrusion issues with the AI-enabled systems and will need to set up dedicated centres for AI development and testing in order to maintain a test-safety regime for systems-of-systems employed using AI. The challenges related to AI use in wars and geopolitical conflicts need to be addressed to generate confidence in the use of such systems. Additionally, testing mechanisms and accuracy standards need to be implemented for system components. Policymakers need to address the operational risks and ethical considerations of employing AI in military systems.

---

[25] Amit Katwala, "**The US Air Force is Turning Old F-16s into Pilotless AI-Powered Fighters"**, *WIRED*, 27 June 2020.

[26] **"Biden Administration Asks US Congress to Approve New Weapons Sales to Turkey"**, *Middle East Eye*, 11 May 2022.

[27] Simona R. Soare, **"Algorithmic Power, NATO and Artificial Intelligence"**, Military Balance Blog, IISS, 19 November 2021.

[28] Ibid.

[29] Simona R. Soare, No. 9.

Conclusion

In future, AI will act as an enabler to out-adapt competitors and adversaries. The current AI strategy of NATO needs to address the vulnerabilities in AI systems and related measures for effectively using autonomous weapon systems and military governance of AI. The NATO accelerator has been devised to address, prioritise, and promote interoperability in transatlantic cooperation to drive the strategic innovation process. The key drivers for Innovation in AI and other EDTs will be the establishment of the NATO-Civil-Military Technology capability that will include various actors from the military, civil, state and private sectors as a part of the EDT innovation ecosystem. Another critical factor is the broadening of the NATO–EU cooperation through a joint taskforce on defence innovation and EDTs to regularise and provide strategic capabilities on ethical and adoption challenges of EDTs like AI and ML.

Furthermore, NATO needs to protect the use of AI from manipulation and disruption and align it with its stated principle of "Responsible use of AI". NATO needs to work on AI adoption challenges centred on innovation and arms control. It can look towards bringing in guiding principles on use of AI-driven lethal autonomous weapon systems. It is expected that in the next 2–3 years, AI's use will be confined to the field of military logistics, reconnaissance, mission planning and support, predictive maintenance of a military facility, data fusion and analysis, cyber defence and optimisation of processes. In the long run, NATO could employ AI for more complex military applications as it generates greater political support for offensive AI military projects.

About the Author

Dr Sanur Sharma is Associate Fellow at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses