Role of Artificial Intelligence in Defence Strategy: Implications for Global and National Security

Ahmad Khan[*], Irteza Imam[**] and Adeela Azam[***]

Abstract

This study analyses the role of Artificial Intelligence (AI) in the defence strategy of high-end technology states and its implications for regional states' national security. The United States (US) in 2014 announced its Third Offset Strategy (TOS) which has conceived the role of AI and Machine Learning (ML) in bringing autonomy to its weapons systems to offset the threats emanating from its adversaries i.e. Russia and China. TOS envisions constant and consistent upgrading of the US forces, tactics and strategies to triumph on the battlefield. The US has been at the forefront to introduce innovations in its modern weaponry and their employment (tactics & strategy). Russia and China are also following the suit. The TOS is based on the development of AI and Lethal Autonomous Weapon Systems (LAWS) which involve human-machine collaborative decision making, assisted human operations, advanced manned-un-manned systems and network enabled autonomous weapons. Apart from the US, Russia and China are also developing similar systems to counter the US' TOS which may result in the new age arms race globally. The paper also analyses the development of LAWS and subsequent prospects of giving autonomy to nuclear forcerelated systems alongside the deterrent value of nuclear weapons might result in future conflicts that may be detrimental to international security and national security of the states.

Keywords: Artificial Intelligence (AI), Machine Learning (ML), Third Offset Strategy (TOS)**,** Lethal Autonomous Weapon Systems (LAWS), US, Russia, China.

[*] *The author is a visiting faculty member at the Department of Strategic Studies, National Defence University, Islamabad.*

[**] *The author is a graduate from the Department of Defence and Strategic Studies, Quaid-e-Azam University, Islamabad.*

[***] *The author is MPhil graduate from the Department of International Relations, Quaid-e-Azam University, Islamabad.*

Introduction

The pioneer of Artificial Intelligence (AI), John McCarthy, defines it as "the science and engineering of making intelligent machines, specially intelligent computer programme."[1] Likewise, "AI is a way of making a computer, a computer-controlled robot, or a software think intelligently, in a similar manner through which an intelligent human thinks and makes decisions."[2] The primary goals of AI are; a) to create expert systems and b) to implement human intelligence in machines.[3]

An intelligent machine or a computer programme can perform expert, mundane and formal tasks. These tasks are financial analysis, engineering, scientific analysis, medical diagnosis (expert tasks), perception common sense reasoning, natural language processing (mundane tasks) and Math and games (formal tasks) respectively.[4]

The role of AI in the US' TOS is extremely important. AI-based military systems and the subsequent utilisation of AI-based decision-making systems is gaining momentum in high-end technology states. In this changing global landscape, the shift of balance of power would be linked to states' acquisition of new technologies. The fourth industrial revolution is rapidly bringing up the revolution in technological affairs where AI and Machine Learning (ML) are becoming part of the weapons systems. AI and ML along with quantum computing are part of the US' TOS and China and Russia are too assertive in this technological revolution. The relevance of nuclear deterrence is challenged with the advent of critical emerging technologies. In this field, the US is developing a "National Security Innovation Base to develop the highest-quality science and technology workforce in the world. At the same time, the US also ensures that its adversaries would not acquire its intellectual property, research, development or technologies."[5] The development of

[1] "What is Artificial Intelligence," Society for the Study of Artificial Intelligence and Simulation of Behaviour, https://www.aisb.org.uk/public-engagement/what-is-ai,
[2] Ibid.
[3] "Artificial Intelligence-Overview," Tutorialspoint, https://www.tutorialspoint.com/artificial_intelligence/artificial_intelligence_overview.htm
[4] Ibid.
[5] *World Leader of Critical and Emerging Technologies* (Washington DC: The White House, October 2020).

critical emerging technologies would ensure the US to induct AI-based weapon systems to bolster its TOS to neutralise the threats emanating from its adversaries. The Biden administration reiterates that China becomes more assertive and Russia remains determined to enhance its global influence.[6] This suggests the revival of great power politics and shifts in the global political landscape. At this crossroad, AI and ML coupled with critical emerging technologies are likely to play a significance in determining the political, strategic and economic influence of the state. The paper explores multiple dimensions of the applications of AI in national defence. For that purpose, the findings of the research are based on deductive reasoning using both qualitative and quantitative methods. The paper aims to find answers to some of the key questions including how TOS will impact the role of nuclear deterrence and how the defence strategies will embed or envision AI and ML in the longer run to counter adversarial threats. Also, the study is primarily a descriptive analysis of the applications of AI in defence strategies of significant military powers with a focus on the US, China, Russia, India and Pakistan.

Machines with Artificial Intelligence

AI demonstrates behaviour akin to human intelligence and if the machine is equipped with AI then it will start learning.[7] ML is described as a machine that can perform functions that are associated with human intelligence including problem-solving, presentation, execution, manipulation, reasoning, social intelligence, interaction and creativity. At present, high-end technology states are taking quantum steps in the areas of AI, ML, drones, robotics, spoofing, jamming etc., to bolster their national defences. This shows the importance of AI and ML in the day to day life as well as maintaining the national defence of the state. The idea of autonomous machines has become a reality in the 21st century.

[6] Renewing America's Advantages: Interim National Security Strategic Guidance (Washington DC: The White House, March 2021), 8.

[7] Thomas McFarland and Reese Parker, *Expert Systems in Education and Training* (New Jersey: Educational Technology Publications, 1990), 11.

Artificial Intelligence in Defence and Strategies

AI has increased the scope of giving intelligence reasoning to machines; as a result, the machines are not only performing tasks but also executing critical decisions — either with or without human supervision. Autonomous machines are performing tasks and executing decisions in several areas like Intelligence Gathering, Surveillance, Reconnaissance (ISR) and Cyber-Security.[8]

AI and ML are dual-use applications that can be used for offensive purposes effectively. The major military powers are employing intelligent systems for better situational awareness. States are chalking out strategies to structure data through cyber means. Likewise, data collected is being used to improve the decision-making process.[9]

Technologically advanced states have step-up their efforts to bring military innovation offering a strategic change in their capability to maintain their military superiority over their adversaries. They are making efforts to introduce AI and ML in their defence system to offset the threats posed by their adversaries, especially those who are not at par with them. They have prioritised the interpretability of autonomous systems, avoiding mishaps and promoting freedom of actions in combat operations in their defence strategies. In response, other major powers have also paced up their quest to compete with arch-rivals in the domain of AI and ML. Their military strategies envision the induction of autonomy and AI to build high-technology arms to fight with technologically advanced weapons.[10]

[8] Peter Roberts and Andrew Payne, "Intelligence, Surveillance and Reconnaissance in 2035 and Beyond," RUSI, RUSI Occasional Paper, February 2016, https://rusi.org/sites/default/files/201602_op_isr_in_2035_and_beyond.pdf;

[9] Madhukar Dayal, Sachin Garg and Rubaina Shrivastave, "Big Data: Road Ahead for India," *Indore Management Journal*6, no.2 (2014): 1-14.

[10] M.L. Cummings, "Artificial Intelligence and the Future of Warfare," The Chatham House, June 1, 2016, https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings.pdf.

Lethality of Weapons and Artificial Intelligence

The evolving nature of warfare and technologies has produced more lethal weapon systems and brought more advancement in the factors contributing to the lethality of the weapons. The new factors are stealth, data-gathering by weapon systems, unmanned systems and evolution of C^4I^2SR over the past four decades. Importantly, the tale of the first and second offset strategies suggests that the US Air Force lacked stealth technology during the height of the Cold War.[11] Likewise, the underwater sea systems were vulnerable to detection and trace by the rival forces.

Trevor Dupuy and his associates at the Historical Evaluation Research Organization (HERO) have assessed Theoretical Lethality Index (TLI) of weapons used on the battlefield over the past four centuries. Table no. 1 shows the lethality of different weapons starting from bow to thermonuclear devices. "The lethality of weapons primarily depends on factors including rate of fire, targets per strike, range, accuracy and reliability."[12] All these factors are assessed to ascertain the potential lethality of a specific weapon.[13]

[11] Arthur Holland Michel, "The Killer Algorithms Nobody's Talking About,"*Foreign Policy*, January 20, 2020.
[12] *Historical Trends Related to Weapon Lethality* (Washington, DC: Historical Evaluation and Research Organization, October 15, 1965).
[13] Trevor Dupuy, *The Evolution of Weapons and Warfare* (New York: The Bobbs-Merrill Company, Inc., 1980).

Table No. 1

Theoretical Lethality Index (TLI)

Weapons	TLI Values
Sword	23
Bow	19
Musket	19
Flintlock	43
Rifle	36
Machine Gun	3463
French 75 mm Gun	386,530
Howitzer	657,215
Tank	935,458
Fighter Bomber	1,245,789
Ballistic Missile	3,338,370
20 KT Nuclear Airburst	49,086,000
One Megaton Nuclear Airburst	694,385,000

Source: Dupuy Institute, November 12, 2016, http://www.dupuyinstitute.org/blog/2016/11/12/what-is-the-relationship-between-rate-of-fire-and-military-effectiveness/

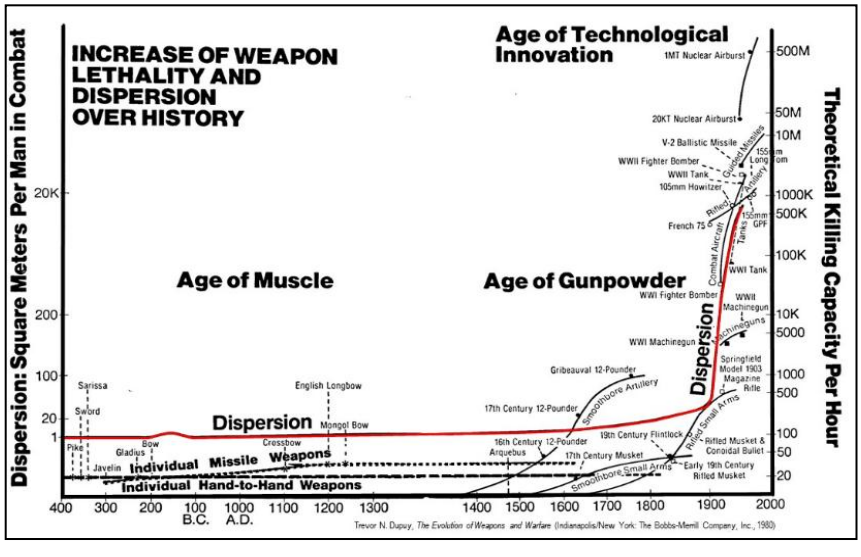
Figure No. 1 shows the graph between dispersion (square metres per man in combat) and potential killing capacity per hour. It is astonishing to note that a one-megaton nuclear weapon has proved to be a more lethal weapon as it has possessed the power of killing the people indiscriminately than any other weapons in the history of warfare. More so, the introduction of a historical secret document of the US Department of Defence (DoD) released in 1979 suggests that "a two-sided nuclear war has never been fought. It is generally conceded that the probability of a nuclear attack on the US and its allies is very low at present."[14] This low probability of fighting a

[14] H. Brown, "The Nuclear Balance," Department of Defence, United States of America, 1979.

nuclear war gives rise to the probability of employment of AI-based weapon systems which are more accurate, lethal, stealthier and precise to acquire targets involving indiscriminate killings per hour. Acquiring this autonomous weapon system can play a vital role in future warfare.

Figure No. 1

Graph between Dispersion of Soldiers and TLI Per Hour



Source: Dupuy Institute, November 12, 2016,http://www.dupuyinstitute.org/blog/2016/11/12/what-is-the-relationship-between-rate-of-fire-and-military-effectiveness/

Lethal Autonomous Weapons Systems (LAWS)

Weapon systems that could identify and attack a target without human intervention are tagged as LAWS. It is estimated that fully autonomous killer robots which fall under the category of LAWS could be developed within 20-30 years. At the moment, the research & development in the field of robotics highlights that these killer robots possess some degree of autonomy and the ability to operate without human intervention or supervision.[15]

[15] "Background on Lethal Autonomous Weapons Systems," United Nations Office for Disarmament Affairs,https://www.un.org/disarmament/geneva/ccw/background-on-lethal-autonomous-weapons-systems/

> The legal understanding of LAWS suggests that human involvement is divided into three categories. First, the Human-in-the-Loop Weapons, category suggests that robots can select targets and deliver force only with a human command. Second, the Human-on-the-Loop Weapons, category suggests that robots that can select targets and deliver force under the oversight of a human operator can override the robots' actions. Third, Human-out-of-the-Loop Weapons, category suggests that robots that are capable of selecting targets and delivering force without any human input or interaction.[16]

All three types of unmanned weapons, in other words, everything from remote-controlled drones to weapons with complete autonomy include robot and robotic systems.

Autonomous Weapons System (AWS) in the contemporary era is mostly akin to science fiction. There is no such existence of fully operational AWS at the moment. However, there is due diligence given to the development of AWS in scientifically advanced countries to develop such weapons. Likewise, states are devising rationale and strategies for the adoption of AWS in their conventional and non-conventional weapon system. However, it is a tough job to ask to install a full operational AWS system in a nuclear-force related system because of several devastating consequences[17] which are as follow:

a) A fully operational AWS would cast destabilising effects on international security.
b) It would incentivise other nuclear weapons states to follow the suit if one nuclear weapon state able to give autonomy to its nuclear force-related system.

[16] "Losing Humanity: The Case Against Killer Robots," Human Rights Watch, November 19, 2012, https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots

[17] Jean-Marc Rickli, "The Impact of Autonomous Weapons Systems on International Security and Strategic Stability," Geneva Centre for Security Policy, January 15, 2018, http://www.css.ethz.ch/en/services/digital-library/articles/article.html/0654ca0d-4883-4b80-a953-9f7749e8162b/pdf; Amos Guiora, "Accountability and Decision Making in Autonomous Warfare: Who is Responsible?" *Utah Law Review*, no.2 (2017): 393-422 and also see, "Autonomous Weapons Systems: Five Key Human Rights Issues for Consideration," Amnesty International, 2015, https://amnestyfr.cdn.prismic.io/amnestyfr%2F3258828f-1127-4b6d-ba92-4681f53ffe26_act3014012015english.pdf

c) It would also provide an opportunity to states to augment strategies of pre-emption to emerge to thwart the use of AWS.

Autonomy in Nuclear Force-Related System

States are exploring avenues to bring autonomy to nuclear force-related systems.[18] However, the emergence of AI-based technologies has increased the chances of misperception and misunderstanding leading toward a strategic trust deficit between nuclear-armed adversaries, lowering the nuclear threshold and luring the states of pre-emption nuclear strikes in war-like situations. States are pursuing AI-based technologies to increase autonomy in the situational awareness system, especially in the Ballistic Missile Defence (BMD) system.[19]

To give autonomy in Nuclear Command and Control (NC^2) systems has become an issue for states which lie low on technology advanced pyramids. NC^2 is an important domain in the nuclear force-related system as it involves precise, accurate, rational and most importantly politically motivated decision-making processes. The debate suggests that states have not completely inducted intelligent machines in their NC^2 systems so far due to the mentioned threats.

AI and US Third Offset Strategy (TOS)

In 2014, the then US Secretary of Defence, Chuck Hegal, set out the US military's quest for a combination of new technologies to maintain the US military supremacy over the next 20 years in the face of Russian and Chinese challenges. TOS envisioned innovative thinking, the development of new operational concepts and new ways of organising and long-term

[18] "For example, while not based on ML technology, the Soviet Union's Dead Hand system in which, under certain conditions, nuclear missiles would be launched without a human in the loop is a known example of nuclear weapon automation." See Hoffman, D. E., *The Dead Hand: The Untold Story of the Cold War Arms Race and Its Dangerous Legacy* (Anchor Books: New York, 2009) quoted in Vincent Boulanin. ed., *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk* (Stockholm: SIPRI, May 2019), 65. Likewise, the potential applications of ML in nuclear-related systems including, missile warning and guidance system and cyber security.

[19] Jonathan Masters, "Ballistic Missile Defence," Council on Foreign Relations, updated August 15, 2014, https://www.cfr.org/backgrounder/ballistic-missile-defense

strategies to offset challenges to the US national security. The strategy is primarily based on bringing autonomy in weapon systems and developing unmanned drones, vehicles and underwater autonomous submarines to achieve military targets on the battlefield. Primarily, TOS is aimed to form a Global Surveillance and Strike (GSS) system. GSS network is aimed to respond to the military modernisation of Russia and China. Besides, GSS is likely to counter the proliferation of critical disruptive technologies and Weapons of Mass Destruction (WMD).[20] According to a DoD report, "the network is a mix of low-end and high-end platforms that could operate across a range of permissive and contested environments, including anti-access/area denial (A2/AD) technologies."[21] TOS is also aimed to project the US global power projection, its military capability and capacity to neutralise the threat emanating from its strategic competitors.[22]

History of Offset Strategies

The revolution in technological affairs provides a rationale for defence policymakers to come up with ideas to neutralise the emerging threats with the employment of emerging technologies. However, it is noticeable that what kind of environment enforces such an idea and for that purpose, the failures in the past must be analysed before they once again become part of the future strategies.

a) First Offset Strategy

The first offset strategy was chalked out at the onset of the Cold War which envisioned the employment of Tactical Nuclear Weapons (TNWs) in Europe to deny the former Soviet Union's overwhelming conventional technological and numerical superiority over allied forces.[23]

[20] "Global Surveillance and Strike," *Inside Defence,* October 27, 2014, https://insidedefense.com/insider/global-surveillance-and-strike.
[21] Ibid.
[22] Freedberg Jr, S. "Hagel Lists Key Technologies For US Military; Launches Offset Strategy," *Breaking Defence,* November 16, 2014, http://breakingdefense.com/2014/11/hagel-launches-offset-strategy-lists-key-technologies/.
[23] Keck, "A Tale of Two Offset Strategies," *The Diplomat,* November 18, 2014, http://thediplomat.com/2014/11/ataleoftwooffsetstrategies/.

The US's strategists envisioned Europe as the future battlefield between the former Soviet Union and NATO allied forces. To equalise the strategic equation, the US' First Offset strategy relied on developing TNWs to offset the fear of a loss of allied forces in the European theatre and to deter a full-scale conventional war that might have escalated to a full-fledged nuclear exchange. During this period, the US designed and deployed numerous battlefield or TNWs such as the very short range "Davy Crockett," the Pershing series of ballistic missiles etc., to stop any attempt by the former Soviet Union armoured forces to break NATO lines in the western Europe. As part of the First Offset strategy, the US also developed long-range bombers capable of targeting the former Soviet Union heartland from bases away from the western Europe.[24]

The First Offset strategy had its limitations as both the US and the former Soviet Union were engaged in high-intensity armed conflicts like in the Korean Peninsula. The US' political administration then started to contemplate a "flexible response" strategy instead of "massive retaliation" to open up its response options in case of conflicts of varying intensities.[25] The failure of the First Offset strategy was primarily because of the US' flawed strategy to counter Soviet conventional forces in the European theatre.

b) The Second Offset Strategy

The Second Offset Strategy commenced during the 1970s.The first phase had considerable technological drawbacks such as the lack of any comprehensive ISR capabilities. The lack of advanced ISR capabilities has led to the US's policy and decision-makers underestimating the former Soviet Union's nuclear capabilities, particularly the advanced and numerically expansive arsenal of Intercontinental Ballistic Missiles (ICBMs).[26]

This strategy was focused on developing the US' space-based ISR capabilities along with Airborne Radars (AWACS) etc. Likewise, the

[24] P Grier, "The First Offset," *Air Force Magazine*, 2016.

[25] Keck, "Tale of Two Offset Strategies."

[26] T Walton, "Securing the Third Offset Strategy: Priorities for the Next Secretary of Defense," *Joint Force Quarterly* 82, (2016): 6-15, http://www.dtic.mil/doctrine/jfq/jfq-82.pdf

strategy also envisioned the development of stealth technology in aircrafts, which gave the US Air Force a clear conventional advantage over all nations.[27]

Core Problems in First and Second Offset Strategies

During the development of the TOS under the Obama administration, four basic threats or problems were identified, these include a.) military infrastructure such as bases whether ports, airfields or ground installation were under threat, b.) naval vessels were easier to detect and hence being engaged, c.) air assets that lack stealth capability was under direct threat due to integrated air defence networks by near-peer adversaries and d.) technological advances by near-peer competitors had diminished the sense of space superiority for the US.

The US military faced the above mentioned operational problems during and after the Cold War which restricted the US to project its military and political power. However, these problems were not proved to be the stumbling block in the US path to becoming a global leader and military power. However, the challenges for the US military dominance are growing especially threats emanating from cyberspace are grave and require a greater response. To counter these weaknesses, the building blocks of the TOS were formulated as it does not give a favourable environment for China and Russia to compete with the US.[28]

Building Blocks of TOS

The building blocks of TOS are primarily accentuating the role of AI in future warfare. AI gives autonomy to machines with and without (limited) human intervention or supervision. An autonomous learning system under TOS will enjoy delegated decision-making power in applications that require fast-than-human reaction time. The human-machine collaborative decision-making process would exploit the advantages of both human and

[27] Ibid.

[28] Timothy Walton, "Security the Third Offset Strategy: Priorities for the Next Secretary of Defence," *Joint Force Quarterly* 82, no. 3 (2016).

machines for better and faster human decisions in a conflict situation.[29] The machine will assist human operations to help humans perform better in combat operations. Also, the advanced manned or unmanned system operations will employ innovative cooperative operations between manned and unmanned platforms. Lastly, the "network-enable, autonomous weapons will operate in future cyber domains which allow for cooperative weapon concepts in communications-denied environments"[30]

Areas of Investment under TOS

To achieve the goals defined under the TOS, the US has started the exploration of potential fields like Biotechnology, Nanotechnology, Robotics, Atomics and Man-machines which require increased government funding and support to effectively develop and employ the TOS. Besides these areas, under TOS, the US is also contemplating further investment in the area of C^4I^2SR, Space Situational Awareness(SSA), protecting space assets, ISR enterprise, development of direct energy weapons (DEWs), autonomous human-machine integration and development and deployment of undersea warfare system and vessels.[31]

China, Russia and India in the Field of AI

AI has undeniably become the centre of international strategic competition. AI is dubbed as an advanced instrument of economic, industrial and technological transformation. Nevertheless, the implications of the use of AI in the military domain would be multi-dimensional. Russian President, Vladimir Putin indicated the forceful impact of AI and stated "whoever

[29] For further reference see, Jeremy Malaki, "Human Machine Collaborative Decision Making in a Complex Optimization System," (M.Sc. diss., United States Air Force Academy, 2003).

[30] Tangney, J. 2016. "Human Systems Roadmap Review," Human and Bioengineered Systems Division, Office of Naval Research.

[31] J Louth, and C. Moelling, "Technological Innovation: The US Third Offset Strategy and the Future Transatlantic Defense," Armament Industry European Research Group, December 2016, 1-16, http://www.iris-france.org/wp-content/uploads/2016/12/ARES-Group-Policy-Paper-US-Third-Offset-Strategy-December2016.pdf

becomes the leader in this sphere will become the ruler of the world."[32] China, Russia, and the US, being the leading countries in the field of AI are believed to harness the AI in the strategic realm of affairs.

Seeing potential military programmes and projects of major countries in the field of AI, military usage of AI-based systems in practice seems unavoidable. Wide implementation of AI in the military domain may lower the military action threshold. Considering the prevailing trend in this field, the world is likely to face another arms race among major states, the AI arms race.

The US Defence Department's 'Strategy to Apply AI' recognised that "other nations, particularly China and Russia, are making significant investments in AI for military purposes."[33] With the release of the following official documents; *New Generation Artificial Intelligence Development Plan* (AIDP) issued by China's State Council in 2017 and *Made in China 2025*, Beijing made an official announcement concerning AI strategy for the new age of competition.[34]

The AIDP acknowledges the evolving strategic environment of international politics while endorsing the growing role of AI. It notes that owing to the evolving and complex nature of security and international politics, China is urged to take the necessary measures, to bridge the gap, in the field of AI by safeguarding its national security interests.[35] Further, the Chinese report encourages the optimal use of AI to an extent of strategic

[32] Matt Field, "China is Rapidly Developing its Military AI Capabilities," *The Bulletin of Atomic Scientists*, February 8, 2019, https://thebulletin.org/2019/02/china-is-rapidly-developing-its-military-ai-capabilities/

[33] Michael T. Klare, "AI Arms Race Gains Speed," Arms Control Association, March 2019, https://www.armscontrol.org/act/2019-03/news/ai-arms-race-gains-speed

[34] Gregory C. Allen, "Understanding China's AI Strategy Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security," Centre for a New American Security, February26, 2019, https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy

[35] Notice of the State Council Issuing the New Generation of Artificial Intelligence Development Plan, State Council Document (2017)No. 35, *The Foundation for Law and International Affairs*, https://flia.org/wp-content/uploads/2017/07/A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf, 2.

decision-making for national defence to strengthen AI-based civil and military systems.[36]

Like other strategic competitors, China is investing in the domain of advanced technologies driven by AI. In doing so, besides Chinese government-owned companies, some private firms are equally delved into research and development. According to Zeng Yi, a senior executive at NORINCO, the third-largest defence company in China, anticipated future battle-grounds being overtaken by LAWS and by 2025 advanced military use of AI will be made.[37] Presently, in addition to developing a range of autonomous military vehicles, Beijing is mainly engrossed to utilise AI to make faster and more accurate decisions.[38]

By contrast to the US and Chinese programmes of advanced technologies and applications of AI, Russia is estimated to be relatively low in advancement and potential in the said field. Generally, Moscow's aspiration for AI is regarded as relatively less ambitious than those of Beijing and Washington. To some scholars, Russia is more likely to compete in other spheres of technology (cyber domain) and conventional arms race rather than competing in the race of AI.[39] This is not to suggest or undermine Moscow's potential in the field, Russia may not be ahead of its strategic competitors, however, it does constitute an AI defence programme. In the domain of military AI, Russia is more focused on robotics.[40]

Russia is believed to set-up organisations dedicated to the expansion of military AI. In March 2018, Russian authorities announced a 10-point AI agenda, aimed at building AI consortium, training and education programme to make advancement in the field of AI.[41] Besides the autonomous system's Moscow plans to integrate AI systems in the maritime

[36] Ibid., 22.

[37] Allen, "Understanding China's AI."

[38] *Artificial Intelligence and National Security* (Washington DC: Congressional Research Service, January30, 2019), 1-30.

[39] Adrian Pecotic, "Whoever Predicts the Future Will Win the AI Arms Race," *Foreign Policy*, March 5, 2019, https://foreignpolicy.com/2019/03/05/whoever-predicts-the-future-correctly-will-win-the-ai-arms-race-russia-china-united-states-artificial-intelligence-defense/

[40]

[41] *Artificial Intelligence and National Security*, 22 & 30.

domain such as introducing unmanned undersea swarming capabilities; aerial, naval and undersea vehicles.[42]

Besides these major states, India has joined this league to use AI. India took a major step in 2018 by constituting a taskforce to examine the associated challenges of AI for India's defence and security. Moreover, India's Defence Research and Development Organization (DRDO) based laboratory, Centre for Artificial Intelligence and Robotics (CAIR) has undertaken a project to harness AI in the defence field. With AI applications, the project is aimed at exploring AI-based solutions to support armed forces to augment desired intelligence, data collection and analysis.[43] CAIR primarily focuses on artificial neural networks, computer vision and situational awareness. However, India's decade-long projects for AI applications have faced constant delays and critique. In comparison to China's advanced progress in the AI domain, India is likely to face a strategic imbalance.[44]

TOS and Competition by Russia and China

Russia and China are also preparing strategies to counter TOS.

a) Russian's Response

Russia is reaffirming its technological advancement in developing Intercontinental Ballistic Missiles (ICBMs), TNWs and modernisation of its nuclear arsenal. All these steps are to counter the US advancement in emerging disruptive technologies and the subsequent development in AI-based technologies. The Advance Russian Force (ARF), is extensively doing research and development on AI, 3d printing and additive technologies, unmanned underwater vessels, DEWS and building industrial

[42] Samuel Bendett, "Red Robots Rising: Behind the Rapid Development of Russian Unmanned Military Systems," The Strategy Bridge, December12, 2017, https://thestrategybridge.org/the-bridge/2017/12/12/red-robots-rising-behind-therapid-development-of-russian-unmanned-military-systems.

[43] "Defence Ministry to Prepare Forces for Use of Artificial Intelligence", *India Today*, January 2, 2019.

[44] Shashi Shekhar Vempati, "India and the Artificial Intelligence Revolution," Carnegie India, August 2016.

partnership with like-minded countries.[45] Moreover, the US and NATO countries believe that Russia has militarised cyberspace. Several cyber attacks on the US institutions and more recently the Solar Winds cyber attack on the US government entities including intelligence agencies networks and nuclear security organisations also originated from Russia. These steps are intended to shift the balance of power in Russian favour by employing cyber technologies. Importantly, Russia is likely to embed and incorporate AI applications with its cyberspace capabilities. This may likely to militarise both fields. As the historical animosity between the two sides continues, Russia would not want to lag behind the US in any of the defence-related capabilities.[46]

b) Chinese Response

China is mastering AI technologies and quantum computing. AI and quantum computing have become one of the top technological and security priorities of China. However, due to language barrier and lack of strategic understanding of Chinese thinking, there is a lack of literature review to highlight what China is really up to in AI, ML and quantum computing. Likewise, China is still to develop a comprehensive rationale to bring autonomy to its NC^2 systems. China is probably likely to follow the Russian and American path to bring autonomy in its nuclear-related weapons system. So far, the Chinese defence and national security policy is based on isolation. Experts argue that China may likely be left alone to bring autonomy to its nuclear systems if any other nuclear weapon system introduces autonomy in its nuclear weapon system. At present, the exceptional part of the Chinese overall response revolves around its space development especially by building its global navigation system, the Beidou. Besides, it is also concentrating on building stealth aircraft. The Chinese response to the US' TOS is linked with its heavy investment in AI-based research and development. China is likely to become a global leader in AI by 2030. It was outlined in its National Artificial Intelligence

[45] V Kashin, and M Raska, "Countering the US Third Offset Strategy: Russian Perspectives, Responses And Challenges," S. Rajaratnam School of International Studies, January 2017.

[46] For further reading see, Stephen Blank and Richard Weitz, eds., *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald* (Carlisle, PA: US Army War College, July 2010)and also see Boulanin ed., *The Impact of Artificial Intelligence*, 65, 66 & 67.

Development Plan released in 2017. Likewise, the US DoD-sponsored reports continue to highlight China's rapid investment, research and development and subsequent induction is aimed to foster and bolster its defence. China's cyber technologies are increasing which it may use as a defence capability in case of an eventuality. It is investing in its next-generation autonomous system and also improving its C^4I^2SR capabilities to counter the US TOS.[47]

Stagnation of Advancement in Quantum Computing

Through quantum computing and AI are distinct technologies, but both will not be developed in isolation from one another. Quantum computers will be able to speed up the machine learning underpinning AI while AI will be able to write algorithms and programmes for quantum computers. However, the lack of advancement in quantum computing is a major obstacle in the advancement in AI-based systems that can be used in nuclear force-related systems.[48]

AI will be vulnerable to hacking, cyber-attacks and commandeering by an intruder if not protected through quantum cyber security. At the moment, there is a technological lag in the development of quantum computing as a result of the advancement establishment of a hack-proof quantum cyber security network has become a distant reality.[49]

Security Implications of AI & ML

According to the views of Stephen Hawking, a renowned physicist, the development of AI has the potential of either being extremely constructive

[47] See for details, Susan Deckar and Christopher Yasiejko, "Forget the Trade War, China Wants to Win Computing Arms Race," *Bloomberg*, April 9, 2018, https://www.bloomberg.com/news/articles/2018-04-08/forget-the-trade-war-china-wants-to-win-the-computing-arms-race; *Military and Security Developments Involving the People's Republic of China 2018* (Washington, DC: Office of Secretary of Defence, 2018); Boulanin (ed), *The Impact of Artificial Intelligence*, 65, 66 & 67.

[48] Arthur Herman and Idalia Friedson, "Quantum Computing: How to Address the National Security Risk," The Hudson Institute, August 2018, https://s3.amazonaws.com/media.hudson.org/files/publications/Quantum18FINAL4.pdf.

[49] Ibid.

or destructive for mankind. Similar views are also shared by leading developers of AI technology and practitioners as well.

a) International Security Implications

Internationally, the inclusion of AI & ML in defence and security affairs may lead to a new arms race that will have far-reaching consequences not only in terms of weapon and capability development but also for strategic stability.[50]

AI and ML when combined with new weapon systems such as hypersonic glide vehicles, precision strike munitions especially in the targeting and command and control mechanisms, can lower nuclear thresholds as the vulnerability of the actor lacking these technologies would increase.[51]

The rapid development and deployment of LAWS is another factor where the proliferation of such weapons may create another security paradigm where attribution is hard. Automation in detection and targeting would also create legal and moral problems that have to be addressed.[52]

b) National Security Implications

There are several risks associated with the introduction of AI and ML in nuclear force-related structure. The specific risks are as follow[53]:

1) AI-based systems may be vulnerable to hacking and cyber-attacks.

[50] Ivan Danilin, "Emerging Technologies and Their Impact on International Relations and Global Security," Hoover Institute, October 3, 2018, https://www.hoover.org/research/emerging-technologies-and-their-impact-international-relations-and-global-security.

[51] Mara Karlin, "The Implications of Artificial intelligence for National Security Strategy," The Brookings, November 1, 2018, https://www.brookings.edu/research/the-implications-of-artificial-intelligence-for-national-security-strategy/.

[52] William Burns et al., "The Rise of Artificial Intelligence: Implications for Military Operations and Privacy," Carnegie Endowment for International Peace, October 31, 2016, https://carnegieendowment.org/2016/10/31/rise-of-artificial-intelligence-implications-for-military-operations-and-privacy-event-5392.

[53] For details, Karlin, "The Implications of Artificial Intelligence."

2) Malicious actors may exploit the vulnerabilities of AI systems deployed by a defender.
3) There are digital, physical and political security challenges to an automated system and in case nuclear force-related system are given autonomy then these above mentioned.
4) Security challenges may be aggravated.

Progress in the AI domain has the potential to bring about a dynamic shift in the national security apparatus that is comparable to the effects brought on by the introduction of aerial warfare, nuclear weapons and computers. These technologies brought considerable changes in the structural organisation, focus, policy and doctrines as well as resource allocation for the US security institutions.[54]

Progress in AI will impact national security by changing the aspects of military, information and economic superiority. The combination of AI and ML would also directly affect the domains of nuclear, aerospace and biotech.

There are multiple ways in which AI could be employed by militaries, these include target identification and engagement, as advances in AI are made, machines (weapon systems) could soon become autonomous and hence the element of accountability and responsibility would erode, resulting in higher chances of escalations and hence destabilising regions and the globe through competition in arms development.

If machines become autonomous then there will likely impact on the nuclear command and control system. At the moment nuclear force-related systems are handed with such autonomy that they will cross the red lines of thresholds. However, there are likely chances that if an AI arms race began between nuclear weapon states then such systems may be developed which take a decision on their own and involve less human and political interference.[55]

[54] For further reference, Danilin, "Emerging Technologies."
[55] See, Burns et al., "The Rise of Artificial Intelligence."

The possibility of an AI arms race between nuclear weapon states cannot be ruled out. This would cause destabilising effects on international security and regional stability. The possible implications are as follow:

1) Induction of LAWS by major nuclear powers.
2) Augmentation of precise and accurate BMD system.
3) Stalemate on AI arms control treaties.
4) Increasing lethality of AI-based conventional weapon system.

Improvements in AI and related technology may also shake up the balance of international power by making it easier for smaller nations and organisations to threaten big powers like the US. Nuclear weapons may be easier than ever to build, but still require resources, technologies, and expertise in relatively short supply.

Conclusion

Autonomy and AI will bring fast, unforeseeable, unexpected and rapid advances in upcoming years due to technological advances involving AI and ML. The states are compelled to adopt AI-based technologies to best prepare to match developments. Efforts are required to counter hostile defence strategies encompassing autonomy and AI including: a.) building technical expertise; b.) developing military research and development resources and taking a fast-follower approach; c.) assessing and tracking the development in hostile states; d.) reducing the chances of misunderstanding, misperception and strategic distrust; e.) examining the lethality of AWS; f.) reducing the friction points in technological, political and diplomatic domains; and g.) learning from past innovations and defence strategies.

It is recommended and advised that the laws and rules governing the development and deployment of AI and Ml in weapons and warfare should be based on best practices and lessons learned from various arms control and arms reduction measures adopted in the 20th Century whether in bilateral or at multilateral forums. These rules and regulations should be drafted within the framework of the UN arms control and disarmament forums so that these are legally binding.

There is a need for new concepts and a clear definition of the threats and ways of combating them. Although it may be hard to achieve, there

is a need to develop laws that prevent the weaponising technologies that mankind depends upon such as cyber and AI.

In conclusion, AI has advantages and disadvantages for humanity. It is clear that if research & development in AI goes unchecked then it would have devastating effects on every field of human life. Likewise, the induction of AI-based weapon systems will likely cause another arms race in the high-end technology states. Furthermore, the countermeasures by the states would be the development of their AI-based weapons system. This would lead to the militarisation of AI, downplaying the positive role AI can play in the future. Likewise, AI will not revolutionise the battlefield, but also change our way of life. At the moment, robots are replacing humans in the industry, thus, creating job insecurity. Likewise, killer robots would be a potential threat to humans. There is no legal instrument or treaty which can restrict the development of killer robots by the developed states. Furthermore, the applications of AI are extensively being used for civil purposes, and it should be noted that AI should not be tainted with negativity. AI has dual use purposes and its civil uses are extremely beneficial for humanity in general. However, its defence applications are extremely dangerous. It is up to the states to decide the utilisation of AI. Lastly, AI is still a human's product.