Artificial Intelligence in Armed Forces: An Analysis

P K Mallick

Introduction

Today is the age of the Fourth Industrial Revolution. The current period of rapid, simultaneous and systemic transformations driven by advances in science is reshaping industries, blurring geographical boundaries, challenging existing regulatory frameworks and even redefining what it means to be human. Artificial Intelligence (AI) is the software engine that drives the Fourth Industrial Revolution. AI is creating targeted marketing, safer travel through self-driving cars, smarter weapons and new efficiencies in manufacturing processes, supply chain management and agricultural production. It holds the promise of solving some of the most pressing issues facing society, but also presents challenges such as inscrutable "black box" algorithms, unethical use of data and potential job displacement.

Artificial intelligence comprises machine programmes that can teach themselves by harnessing High Power Computing(HPC) and big data, and eventually mimic how the human brain thinks, supports and enables nearly every sector of the modern economy. Corporations and governments are fiercely competing because whoever is the frontrunner in AI research and applications will accrue the highest profits in this fast

Major General **P K Mallick** VSM (Retd) was a Senior Directing Staff (SDS) at the National Defence College, New Delhi.

growing market and gain a military technological edge. AI itself will not manifest just as a weapon. It is an enabler that can support a broad spectrum of technologies.[1]

These technologies are starting to have a transformative effect on defence capability. AI will have digital, physical and political security implications, expanding existing threats, introducing new threats and changing the character of threats and of war. These changes could include the automation of social engineering attacks, vulnerability discovery, influence campaigns, terrorist repurposing of commercial AI systems, increased scale of attacks, and manipulation of information availability. This has caused countries around the world to become increasingly aware of the impact of AI. There has been tremendous activity concerning AI policy positions and the development of an AI ecosystem in different countries over the last 18 to 24 months. To cite a few examples, the US published its AI report in December 2016; France published its AI strategy in January 2017 followed by a detailed policy document in March 2018; Japan released a document in March 2017; China published its AI strategy in July 2017; India published a Task Force report in August 2017, and the UK released its industrial strategy in November 2017.

Global investments in artificial intelligence for economic and national security purposes are increasingly being described as an arms race. The character of AI technology, like robotics, makes many countries well-positioned to design and deploy it for military purposes. In Southeast Asia, Singapore is on the cutting edge of AI investments (both military and non-military). In the military domain, South Korea has developed the SGR-A1, a semi-autonomous weapon system designed to protect the demilitarised zone from attack by North Korea and others.

This explains that AI is increasingly becoming a key component of national security. As India's 2017 Task Force report states:[2] "AI can be a force-multiplier for several national security missions. Potential applications include Autonomous Underwater Vehicles (AUVs) and

Unmanned Combat Aerial Vehicles (UCAVs) for underwater and aerial defence operations as well as coastal and border surveillance; robot mules for unburdening soldiers; robots for counter-IED and counter-terrorism operations and close-in-protection systems against cruise missiles and similar aerial threats […]".[3] In view of this, national security imperatives require that technology-based force multipliers be developed. In doing so, some areas where AI-based systems could be usefully deployed are: autonomous surveillance and combat systems, adaptive communications systems, AI-based cyber attack mitigation and counter-attack systems and, multi-sensor data fusion-based decision-making systems.

Changing Nature and Character of War

Military professionals swear by the maxim given by Carl von Clausewitz that "war's nature does not change—only its character". The former describes 'what war is' and the latter describes 'how it is actually fought'. From a Clausewitzian perspective, that war is human fundamentally defines its nature.[4] In view of this, war's nature is violent, interactive and fundamentally political. However, the character of war describes the changing way that war as a phenomenon manifests in the real world. War's conduct is undoubtedly influenced by technology, law, ethics, culture, methods of social, political, and military organisation and other factors that change across time and place.[5] The character of warfare changes in "concert with the tools that become available and how they influence the ways militaries organise themselves to fight wars".[6]

There is an argument that AI has the potential to go beyond shaping the character of war and change the nature of war itself. The key query posed is: can AI alter the nature of war itself because wars will be fought by robotic systems, not people, and because of AI's potential to engage in planning and decision-making that were previously human endeavours?[7] To which, US Defence Secretary James Mattis speculated in February 2018 that AI is "fundamentally different" in ways that raise questions

about the nature of war.[8] Former US Deputy Secretary of Defence Robert O. Work said, "Rapid advances in artificial intelligence and the vastly improved autonomous systems and operations they will enable are pointing towards new and more novel war-fighting applications involving human-machine collaboration and combat teaming".[9] The role of educated humans will begin to concentrate on the higher cognitive tasks of processes such as mission analysis, operational planning, and assessments. More specifically, in relation to future conflict, as ambiguity will increase despite interconnectedness, the velocity and scale of activity will make it difficult to discern the important from the unimportant and the real from the fake. In this scenario, adversary spoofing, deception and data manipulation and corruption will create a common operational picture that is part fact, part fiction. This uncertainty in situational awareness will feed decision cycles that will be compressed by pervasive data and near instantaneous communications.

With these systemic changes, the character of warfare will clearly change, and these changes could significantly influence the Clausewitzian elements that frame our understanding of war's nature. However, autonomy will change the nature of war in several ways, as suggested:[10] (a) It could weaken the role of political direction by forcing response delegation to lower echelons for faster forms of attack. (b) Autonomy can lessen the ability of governments to gain the support and legitimacy of their populations, while making it easier for foreign governments to manipulate their adversary's populations. (c) Deep learning forms of AI will augment the intuition and judgment of experienced commanders. (d) Automated technologies could reduce popular support for professional military institutions, which, paradoxically, could free governments to employ force more readily since the political consequences are reduced. (e) As with the earlier ages, friction and uncertainty will endure. (f) The age of autonomy can introduce new forms of friction while reducing human factors in tactical contexts. To which, the most significant elements of

"war, violence, human factors, and chance, will certainly remain", and "so too, will fog and friction".[11] War's essence as politically directed violence will remain its most enduring aspect, even if more machines are involved at every level. As technology advances at a rapid pace, the nature and character of war will be changed. In the upcoming military revolution of autonomy, we will have to consider new sources of combat power and assess how they impact each level of war.[12]

Given this changing nature of warfare, the US Department of Defence (DoD) has developed a multi-decade strategy for applying a suite of advanced technologies to nearly every facet of its operations. In the first phase, the DoD will create a more intelligent force, using AI to enhance platforms, munitions and decision processes. As these technologies mature, the US aims to create a more autonomous force, pairing AI enabled systems with human military personnel to accentuate the strengths of each, enabling faster decisions and better combat outcomes. In the more distant future, "swarms" of advanced cognitive robots may redefine combat operations in the battle space, as explained in Fig 1 below.

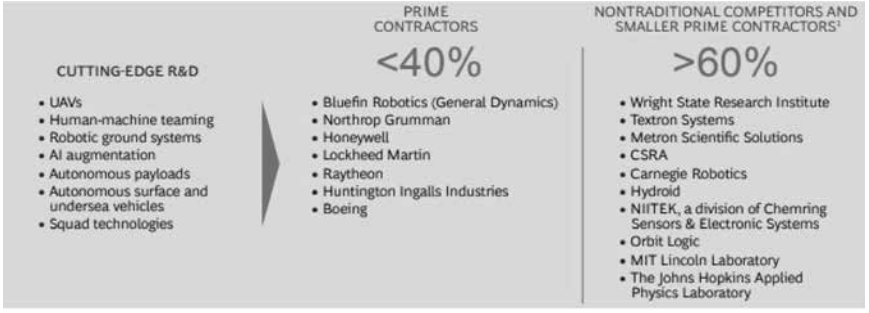
Fig 1: Assessment of the Impact of AI and Robotics on Future US Military Operations

		SAMPLE APPLICATIONS				
		LAND	SEA	AIR	SPACE	CYBER
US battle network	Sensors	• Sensor-laden robotic ground vehicles	• Long-endurance autonomous surveillance	• Sensing distributed to "attritable," or unmanned, wingmen	• AI-enhanced situational awareness in space	• AI-enabled cyber-monitoring and triage
	Command, control, communications, and intelligence	• Autonomous AI processing • Cooperative human-machine interfaces and augmented decision making				
	Effects	• Armed ground vehicles • Intelligent nonkinetic engagement	• Autonomous "swarms" of small robotic platforms • Systems to counter UAVs, surface swarms	• Attritable wingmen capable of conducting air-to-air combat	• Autonomous antisatellite counter-measures	• AI-enabled cyberoffense and cyberdefense
	Logistics	• Autonomous support (for example, pack robots, resupply systems, and aerial refueling UAVs) • Modernized distribution centers optimized with warehouse robots, industrial Internet of Things, and big data				
Force delivery (for example, training)		• Physical or virtual autonomous systems for use in training • Greater demand for simulation equipment and services				

Source: Eric Gons et al. (2018).[13]

The DoD is bringing in key technologies from commercial industry, increasing the scope of competition that prime contractors face. Prime contractors may be tempted to cede the AI and robotics market to small niche players or sub-contractors. More than 60 per cent of the robotics focussed contracts in the President's Budget for Fiscal Year 2017 were awarded to non-traditional defence players or small prime contractors, as shown in Fig 2 below.

Fig 2: Estimated Share of Programmes for Unmanned, or Autonomous Technologies



Source: Eric Gons et al. (2018).[14]

What makes AI significant is the fact that it can operate in several dimensions, such as:

- It can be used to direct physical objects, such as robotic systems, to act without human supervision. Whether in tanks, planes or ships, AI can help reduce the need to use humans, even remotely, or as part of human machine teams. Swarm techniques generally involve the creation of supervised algorithms that direct platforms such as drones.
- AI can assist in processing and interpreting information. Image recognition algorithms can be used for tagging. Project Maven is a US military programme that seeks to develop algorithms to automate the process of analysing video feeds captured by drones.

- Overlapping narrow AI systems could be used for new forms of command and control, operational systems, including battle management, that analyse large sets of data and make forecasts to direct human action or action by algorithms.
- Future AI systems offer the potential to continue maximising the advantages of information superiority, while overcoming the limits in human cognitive abilities. AI systems, with their near endless and faultless memory, lack of emotional investment and potentially unbiased analyses, may continue to complement future military leaders with competitive cognitive advantages.

Given the multi-dimensional nature of AI, its emerging significance will be played out in the following areas:[15]

First, military exploitation of AI and autonomous systems is inevitable. The challenges and realities of big data, complex networks and systems, uncertain environments, ubiquitous and intense peer competition are drivers in both the commercial and military spaces and steer each toward a common set of solutions. Once advanced AI is achieved, it will quickly spiral into almost every area of the commercial, governmental and military domains.

Second, early adoption of AI enabled technology is critical because potential adversaries will develop and field capabilities without constraint. These leap ahead capabilities could be so game changing that the difference between finishing first and finishing next could mean years of decisive advantage in every meaningful area of warfare. The legacy combat systems, even with version improvements and upgrades, may well be rendered outmatched and ineffective by AI-enabled unmanned autonomous systems, cyber dominance and swarms.

Third, significant acquisition, budget, and cultural inertia exists which could impact the Army's ability to gain advantages with AI technologies. The armed forces currently take a risk adverse approach to acquisition and

requirements, waiting for technologies to mature before prototyping and experimentation. In order for the armed forces to become an innovative organisation, they must promote an innovative culture, accept risk and leverage new ideas, while collaborating and partnering on experiments to enhance creativity.

Fourth, leader development for AI technologies must begin now. The current Army leadership requirements model addresses leader development focussed on human-to-human relationships, but the future will challenge leaders with more human-machine relationships.

Fifth, the moral considerations of AI technologies should be addressed before the technology matures. AI technologies increasingly remove the soldier from the conflict. The Army must begin to mitigate the potential harmful impacts of these technologies now. Operators of unmanned and semi-autonomous systems must understand how the AI processes moral dilemmas, the potential ethical shortcomings of these decisions, and how to ensure ethical decisions are made.

This explains that by distancing the human from conflict, technology lowers not only the costs and risks associated with war, but the political bar to initiating hostilities as well. Legacy attributes of the Army such as flexibility, mobility and expeditionary skills may be replaced by new attributes such as predictive, continuously learning, unknowable, decentralised and compelling. These AI technologies have the potential to change the character of conflict.

Effect of AI Technology on Warfare

Sophisticated AI programmes can now manipulate sounds, images and videos, creating impersonations that are often impossible to distinguish from the original. Deep learning algorithms can, with surprising accuracy, read human lips, synthesise speech and, to some extent, simulate facial expressions. Given the emerging role of AI technologies, their effect is most potent in the field of warfare, wherein the areas to witness the impact are:

- **Intelligence, Surveillance, and Reconnaissance:** Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) are reaching new heights of efficiency that enable data collection and processing at an unprecedented scale and speed. AI is useful in intelligence due to the large data sets available for analysis and helps automate the work of human analysts who currently spend hours sifting through videos for actionable information.
- **Military Drones for Surveillance:** Military units across the world are employing drones to: (a) channel remote communication, both video and audio, to ground troops and to military bases; (b) track enemy movement and conduct reconnaissance in unknown areas of a war zone; (c) assist with mitigation procedures after a war by searching for lost or injured soldiers and giving recovery insights for a terrain and; (d) aid with operations like peace-keeping and border surveillance. While drones help in guarding aerial zones, robots can be deployed on land to assist soldiers in ground operations. Robot fleets function like soldier units and carry out collaborated armed activities using multiple techniques. They are self-reliant, adaptable, and have their fault tolerant systems, all of which contribute to their ability to make and execute decisions swiftly and competently.
- **AI-Assisted Decision-Making:** AI assisted decision-making could help leaders at all levels rapidly design, plan and evaluate operations. Through a continuous deliberative planning process, the AI could update and evaluate the plans against the operational environment. The AI would continuously monitor the environment and warn planners when assumptions are no longer valid or if there is an opportunity to improve the plans. The true power of AI will be in the teaming of the human mind with the AI mind. This type of man-machine teaming will combine human strengths of goal setting, creativity, and ethical thinking with AI strengthening the rational thought through self-taught experience, intuition and deep forecasting.

- **AI-Assisted Common Operating Picture (COP):** AI would catalogue and display a disposition of friendly and enemy forces, automatically built and updated through a big data approach. Despite incomplete intelligence, an AI supported COP could tell where an enemy should be with a corresponding level of confidence. In real time, the AI would continuously interpret the situation, explore multiple lines of effort and determine which is most likely to meet the given success criteria. Based on this, the COP would recommend the next actions and predict likely enemy responses.[16]
- **Cyber Space:** AI systems play a powerful role in cyber space for both defensive and offensive measures. AI systems can perform predictive analytics to anticipate cyber attacks by generating dynamic threat models from available data sources that are voluminous, ever-changing and often incomplete. These data include the topology and state of network nodes, links, equipment, architecture, protocols and networks. AI may be the most effective approach to interpreting these data, proactively identifying vulnerabilities and taking action to prevent or mitigate future attacks.
- **Logistics:** AI is expected to play a crucial role in military logistics and transport. The effective transportation of goods, ammunition, armaments, and troops is an essential component of successful military operations. AI has the potential to help the larger Army reshape its tooth-to-tail ratio and free up additional soldiers for critical areas like combat arms and intelligence, surveillance and reconnaissance.
- **Intelligence:** The Intelligence Community (IC) faces daunting challenges of volume and velocity as well as an everincreasing complexity of variety of data.[17] This results in an inability to fuse data to create multi-sourced intelligence as early in the intelligence cycle and as close to the point of collection as possible. In this regard, AI and machine learning will be instrumental in increasing the effectiveness of the future intelligence analyst workforce, improving the odds of

gaining and sustaining a competitive or temporal advantage. Digital transformation, methodical multi-domain data integration, and algorithmic warfare will be the heart of the intelligence enterprise's role in sustaining a long-term competitive advantage.[18] In doing so, intelligence challenges should be addressed in a two-fold way: embracing machine-learning algorithms that can parse data, learn from the data, and then respond and, encouraging creativity and deep thinking by intelligence professionals.[19]

- **Autonomous Weapons Systems (AWS):** AWS offer potential advantages in future warfare but also present many legal and ethical challenges in addition to the inherent risk in turning over decision-making to machines. Queries such as, if an AWS engages and kills civilians, then who is responsible? What role does the military perform in making ethical decisions if machines and algorithms are executing them? In this regard, the ethical question of whether or not Lethal Autonomous Weapons Systems (LAWS) should be permitted to make life and death decisions is receiving much attention. Several countries continue to develop LAWS that would be capable of completely independent operation if desired. In view of this, the Vice Chairman of the Joint Chiefs of Staff, US Air Force, Gen Paul Selva, has argued that humans should be kept in the decision-making loop. The UK's Foreign Office did not support an explicit prohibition on the use of LAWS because it felt International Humanitarian Law (IHL) provided sufficient regulation. The UK armed forces, however, only operate weapons systems that are subject to human oversight and control.
- **Drones:** The recent drone attack on Venezuelan President Nicolas Maduro has brought to the fore a new aspect of terror attack by unmanned aircraft. This incident suggests how easy drones are to use and how difficult they are to defend against. The use of weaponised drones by lone individuals and small groups, some acting as proxies of nation-states, is no longer just a concern for the future, but also

very much for the present.[20] Countries are now using armed drones in combat—Nigeria, Pakistan, and Turkey have recently done so—and the chances for sophisticated drone technology getting into the wrong hands increases exponentially.[21] If a terrorist group can steal or purchase a drone from a rogue state or corrupt military or intelligence officials, then they could rely on the myriad online videos posted that essentially demonstrate how these unmanned systems may be used to conduct an attack.[22]

- **Swarms:** Specifically, with the armed forces, the advantage lies in adopting a 'swarm mindset'. To argue, such a change would largely be seen in the movement away from the single, exquisite weapons platforms to those that are small, cheap, unmanned, expendable and fast. There are many operational advantages of swarms in terms of autonomy, quantity and speed. Unmanned systems can take greater risks by reducing survivability while maintaining lethality and increasing deployability.

AI in Indian Context

At the event of the DefExpo on April 11, 2018, Indian Prime Minister Narendra Modi categorically stated that "[n]ew and emerging technologies like AI and robotics will perhaps be the most important determinants of defensive and offensive capabilities for any defence force in the future. India, with its leadership in the information technology domain, would strive to use this technology tilt to its advantage".[23] This reflects India's inclination to develop artificial intelligence-based weapon and surveillance systems for future use.

Owing to the emerging role of AI in national security, the 2017 Task Force report has made some significant propositions:[24] First, a consortium of Micro, Small and Medium Enterprises (MSME) industries to be created for the development of autonomous systems such as Unmanned Aerial Vehicles (UAVs) and Underwater Unmanned Vehicles

(UUVs), including sub-systems and components. Second, provision of grants, realistic data and cyber security tools to develop methodologies for protecting digital assets and data from external cyber threats and attacks. Third, existing infrastructure, including the National Intelligence Grid (NATGRID), Human Intelligence (HUMINT), Signal Intelligence (SIGINT), Communication Intelligence (COMINT), imagery data and video surveillance from aircraft, Closed Circuit Television (CCTV) data from urban areas and critical infrastructure locations, and radar data and satellite imagery to be integrated on a unified platform. This suggests that India seeks to embed AI-based techniques in the backbone of the platform to provide need-based real-time information to various security agencies involved in threat mitigation.

Although there is no official military strategy document on the usage of AI in the battlefield, there are several potential applications in the "low-hanging fruit." Among these applications are logistics and supply chain management, cyber operations, intelligence and reconnaissance.[25] Furthermore, Research and Development (R&D) on defence applications of AI is conducted under the Centre for Artificial Intelligence and Robotics (CAIR), established by the Defence Research and Development Organisation (DRDO) in 1986. Over three decades, CAIR has worked on building integrated, networked information systems, data mining tools, robotics, and other AI-enabled products for the Indian military.

For India, AI would significantly help improve the ability of Indian forces to secure the 8,600 miles of land border it shares with other countries. For instance, the Border Security Force (BSF) is working on a pilot programme called the Comprehensive Integrated Border Management System (CIBMS), which would put in place an electronic surveillance system monitored by BSF personnel. Similarly, integrating AI-enabled image recognition and automated alerts into the system would greatly aid in the speed and efficiency of a BSF response.

Another practical application of AI is in improving battlefield operations using all-terrain reconnaissance. In February 2018, the DRDO successfully tested the Rustom 2 UAV, and is reportedly developing a "Multi-Agent Robotics Framework" (MARF), a system that will enable the Indian Army's many battlefield robots to collaborate with each other on surveillance and reconnaissance. Likewise, the DRDO is also developing Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) UAVs to detect radiation, as well as Remotely Operated Vehicles (ROVs) for surveillance and Improvised Explosive Device (IED) disposal.

In order to fully exploit their potential, the Indian military needs to build a close working relationship with the vibrant private technology sector in India, and especially with start-ups working in the AI domain. However, this will involve handing over potentially sensitive data to private firms so as to enable the building of AI systems that can meet the specific needs of the Indian armed forces. This is entirely an uncharted territory. In view of this, to assuage the valid concerns that may arise with sensitive data being in private hands, a unique legal 'trust model' needs to be built that accounts for the needs of the military and technological innovation. While the development of such a model may, in fact, prove to be a tougher task than the simple integration of AI technologies, it needs to be done if the Indian military is to prepare itself for warfare in the 21st century.[26]

Conclusion

Big-data analysis and machine-learning algorithms are already available and vastly expand information processing capabilities. AI is already a military reality. Automated decision-making will play an increased role at every level of the command and control process, from swarming miniature UAVs to the national command authority. Genuine AI in the scientific sense may still be years away, but it is not too early to begin establishing normative limits for LAWS through IHL and military rules of engagement, in anticipation of this eventuality.[27]

In addition to these battlefield roles, AI will transform other military activities, including logistics, intelligence and surveillance and even weapons design. Collectively, these activities, mostly tactical in nature, will have a transformative effect on the strategy of those states employing them. This is because militaries that can successfully develop and utilise them will experience a dramatic increase in fighting power relative to those that cannot.

At present, many pertinent AI technologies are immature. Modern unmanned aircraft in service can operate autonomously, but cannot yet execute the sorts of complex missions that manned equivalents can achieve. Land robots are clumsy on uneven terrain. Sceptics rightly point to previous bursts of enthusiasm for AI, followed invariably by disappointment and stagnation as concepts fail to deliver significant breakthroughs in autonomous decision-making. There is considerable wariness that the hype and publicity surrounding deep learning will not pan out as dramatic breakthroughs. Nevertheless, the rapid progress in AI research, especially of hybrid approaches that utilise multiple AI techniques, along with increasingly powerful hardware on which to run algorithms, suggests the potential for AI to significantly affect existing military activities in the short to medium term, even if it falls short of simulating human level cognition any time soon.

Technological innovations could have large scale consequences for the global balance of power and international conflict. Yet their impact is generally determined by how people and organisations use the technology rather than by the technology itself. Militaries around the world will have to grapple with how to change recruiting and promotion policies to empower soldiers who understand algorithms and coding, as well as potential shifts in force structure to take advantage of AI-based coordination on the battlefield. It is too early to tell what the impact of AI will be, but technology development suggests it will have at least some effect.

Notes

1. Manju Bansal, "AI is the New Black," *MIT Technology Review*, February 27, 2017, at https://www.technologyreview.com/s/603748/ai-is-the-new-black/.
2. Department of Industrial Policy and Promotion, "Report of the Artificial Intelligence Task Force", August 2017, at http://dipp.nic.in/whats-new/report-task-force-artificial-intelligence.
3. Ibid., p. 6.
4. Michael E. Howard and Peter Paret, eds., *On War: Carl von Clausewitz* (Princeton, NJ: Princeton University Press, 1989).
5. F. G. Hoffman, "Exploring War's Character and Nature: Will War's Nature Change in the Seventh Military Revolution", *Parameters*, Vol. 47, No. 4, 2017, p. 23, at https://ssi.armywarcollege.edu/pubs/parameters/issues/Winter_2017-18/5_Hoffman.pdf
6. Michael C. Horowitz, "Artificial Intelligence, International Competition and the Balance of Power", *Texas National Security Review*, Vol. 1, No. 3, May 2018, pp. 46-47, at file:///C:/Users/JASH/Downloads/TNSR-Vol-1-Iss-3_Horowitz.pdf.
7. Ibid., p. 47.
8. Ibid.
9. Robert O. Work and Shawn Brimley, "20YY: Preparing for War in the Robotic Age", Centre for a New American Security, January 2014, at https://fortunascorner.com/wp-content/uploads/2014/05/cnas_20yy_workbrimley.pdf.
10. Kareem Ayoub and Kenneth Payne, "Strategy in the Age of Artificial Intelligence", *Journal of Strategic Studies*, Vol. 39, No. 5-6, 2016, pp. 793-819.
11. Hoffman, n. 5, p. 31.
12. Ibid.
13. Cited in Eric Gons et al., eds., "How AI and Robotics will Disrupt the Defense Industry", *The Boston Consulting Group*, 2018, p. 2, at http://k1.caict.ac.cn/yjts/qqzkgz/zksl/201804/P020180426375927121069.pdf.
14. Ibid., p. 3.
15. See "The Operational Environment and Changing Character of Future Warfare", at http://www.arcic.army.mil/App_Documents/The-Operational-Environment-and-the-Changing-Character-of-Future-Warfare.pdf.
16. Sean Kimmons, "With Multi-Domain Concept, Army Aims for 'Windows of Superiority'", U.S. Army, November 14, 2016, at https://www.army.mil/article/178137/with_multi_domain_concept_army_aims_for_windows_of_superiority.
17. The IC is challenged to acquire, manage, correlate, fuse, and analyse ever increasing amounts of data across agencies. Data in the IC are generated in too many diverse formats, in too many disconnected or inaccessible systems, without standardised structures and without overarching agreed upon ontology. This situation risks wasted collections, lack of timeliness, missed indications and warnings and lack of relevance for decision-making.
18. Cortney Weinbaum and John N.T. Shanahan, "Intelligence in a Data-Driven Age", *Joint Force Quarterly*, Vol. 90, 2018, at http://ndupress.ndu.edu/Portals/68/Documents/

jfq/jfq-90/jfq-90_4-9_Weinbaum-Shanahan.pdf?ver=2018-04-11-125441-307.

19. The following actions need to be taken: intelligence analysts need to be trained on how to recognise attempts by an adversary to use altered or manipulated data, including understanding how to use AI to maximum advantage to prevent even the more sophisticated influence operations from affecting the desired operational outcomes. Data should not be treated as an IT problem; instead, IT systems should be framed by the operational problems they solve. Rapid data access requires effective data management, which calls for new skill sets and expertise, such as data architects and data scientists. Network access across all security domains, access to all relevant data types and agile integration of disruptive technologies are key to achieving and sustaining decision advantage. Publicly available information and open source information will provide the first layer of the foundation of our intelligence knowledge.
20. Lone actors or small cells of terrorists, criminals, or insurgents can effectively harness the tactical flexibility of a small drone to wreak havoc, including potentially using a drone to take down an airliner. State sponsorship of terrorist groups also increases the likelihood of drone attacks, since states can provide the necessary equipment and training, ensuring that terrorist attacks featuring weaponised drones is a near fait accompli in the not so distant future.
21. Colin P. Clarke, "Approaching a ;New Normal': What the Drone Attack in Venezuela Portends", Foreign Policy Research Institute, August 13, 2018, at https://www.fpri.org/article/2018/08/approaching-a-new-normal-what-the-drone-attack-in-venezuela-portends/
22. A scenario universally feared by law enforcement and security services is the use of a small drone to deliver chemical or biological agents in an attack.The possibility that drones could be used to disperse deadly agents or viruses over a sports stadium or public gathering place is a harrowing prospect. See Ibid..
23. Quoted in "India Looking to Step up its AI Game in Defence", *Dailyhunt*, July 06, 2018, at https://m.dailyhunt.in/news/india/english/business+world-epaper-bizworld/india+looking+to+step+up+its+ai+game+in+defence-newsid-91709767.
24. n. 2.
25. R. Shashank Reddy, "How AI can Help the Indian Armed Forces", *Livemint*, March 05, 2018, athttps://www.livemint.com/Opinion/EzKziDVFvruJ0KLJF7ySQM/How-AI-can-help-the-Indian-Armed-Forces.html
26. Amber Sinha et al., "AI in India: A Policy Agenda", The Centre for Internet and Society, September 05, 2018, athttps://cis-india.org/internet-governance/blog/ai-in-india-a-policy-agenda.
27. Kenneth Payne, "Artificial Intelligence: A Revolution in Strategic Affairs?", *Survival: Global Politics and Strategy*, Vol. 60, No. 5, October–November 2018, pp. 7-32, at https://www.iiss.org/publications/survival/2018/survival-global-politics-and-strategy-octobernovember-2018/605-02-payne.