Artificial Intelligence in Military Operations

A Raging Debate and Way Forward for the Indian Armed Forces

Artificial Intelligence in Military Operations

A Raging Debate and Way Forward for the Indian Armed Forces

Lt Gen (Dr) R S Panwar, AVSM, SM, VSM (Retd)

(Established 1870)

United Service Institution of India

New Delhi (India)

Vij Books India Pvt Ltd

New Delhi (India)

Published by

Vij Books India Pvt Ltd
(Publishers, Distributors & Importers)
2/19, Ansari Road
Delhi – 110 002
Phones: 91-11-43596460, 91-11-47340674
e-mail: vijbooks@rediffmail.com
web : www.vijbooks.com

First Published in India in 2018

ISBN: 978-93-

Price : ₹ 195/-

CONTENTS

List of Abbreviations

AI	Artificial Intelligence
RMA	Revolution in Military Affairs
LAWS	Lethal Autonomous Weapon Systems
HRW	Human Rights Watch
MHC	Meaningful Human Control
UNODA	United Nations Office of Disarmament Affairs
CCW	Convention on Certain Conventional Weapons
GGE	Group of Governmental Experts
IHRC	International Human Rights Clinic
IHL	International Humanitarian Law
AI/AS	Artificial Intelligence/ Autonomous Systems
AWS	Autonomous Weapon Systems
ICRC	International Committee of the Red Cross
4GW	Fourth Generation Warfare
DoD	US Department of Defence
SEAD	Suppression of Enemy Air Defences
ICT	Information and Communication Technologies
RMA	Revolution in Military Affairs
IED	Improvised Explosive Devices
UAV	Unmanned Aerial Vehicles
IB	International Border

LoC	Line of Control
CI	Counter-Insurgency
CT	Counter-Terrorism
ISR	Intelligence, Surveillance, and Reconnaissance
DSB	Defense Science Board
PLA	People's Liberation Army
MoD	Ministry of Defence
DARPA	US Defence Advanced Projects Research Agency
N-AIM	National AI Mission
DRDO	Defence Research & Development Organisation
ISRO	Indian Space Research Organisation
CAIR	Centre for Artificial Intelligence and Robotics
UGV	Unmanned Ground Vehicle
MARF	Multi Agent Robotics Framework
MIC	Military-Industrial Complex
DPrP2018	Draft Defence Production Policy 2018
CoEs	Centres of Excellence
DPP 2016	Defence Procurement Procedure 2016
MSMEs	Micro, Small and Medium Enterprises
RFP	Request For Proposal
IDDM	Indian Designed, Developed and Manufactured
JUMP	Joint University Microelectronics Program
ATB	Army Technology Board
ARTRAC	Army Training Command
ADB	Army Design Bureau

HQ IDS	HQ Integrated Defence Services
LTIPP	Long Term Integrated Perspective Plan
SCAP	Services Capital Acquisition Plan
AAP	Annual Acquisition Plan
TPCR	Technology Perspective and Capability Road map
MBT	Main Battle Tank
NCW	Network Centric Warfare
IO	Information Operations
SHQ	Service Headquarters
PMU	Project Management Unit
TCS	Tactical Communication System
US Army RDECOM	the US Army Research, Development and Engineering Command
CERDEC	Communications-Electronics RDE Centre
ARL	Army Research Laboratory
WESEE	Weapons and Electronics Systems Engineering Establishment
IA	Indian Army
MCTE	Military College of Telecommunication Engineering
MCEME	Military College of Electrical and Mechanical Engineers
IN	Indian Navy
IAF	Indian Air Force

ARTIFICIAL INTELLIGENCE IN MILITARY OPERATIONS

A Raging Debate, and Way Forward for the Indian Armed Forces

INTRODUCTION

Artificial Intelligence (AI) has become a field of intense importance and high potential within the defence community. AI technologies hold great promise for aiding military decisions, minimising human causalities and enhancing the combat effectiveness of forces, and in the process dramatically transforming, if not revolutionising, the nature of military systems. This is especially true in a wartime environment, when data overload is often encountered, decision periods are short, and timely and effective decisions are imperative.

Robotic systems are now widely present on the modern battlefield. Increasing levels of autonomy are being seen in systems which are already fielded or are under development, which includes systems capable of autonomously performing their own search, detect, evaluate, track, engage and kill assessment functions, fire-and-forget munitions, loitering torpedoes, and intelligent anti-submarine or anti-tank mines, among numerous other examples. In view of these developments, many now consider AI & Robotics technologies as having the potential to trigger a new Revolution in Military Affairs (RMA), especially as Lethal Autonomous Weapon Systems (LAWS) continue to become increasingly sophisticated.

As a reaction to these developments, for almost five years now a raging debate is on world-wide on the ethical, moral and legal aspects of deploying fully autonomous, AI powered

LAWS in future wars, sensationally dubbed as "killer robots" by human rights advocacy groups. The Campaign to Stop Killer Robots commenced in April 2013 under the aegis of Human Rights Watch (HRW), with the aim of pre-emptively banning fully autonomous lethal weapons, defined as autonomous weapon systems without Meaningful Human Control (MHC). The campaign has been advocating the view that retaining human control over the use of force is a moral imperative and essential to promote compliance with international law and ensure accountability.

Triggered by this campaign, nations have been discussing this issue for the last four years at the United Nations Office of Disarmament Affairs (UNODA) forum on Convention on Certain Conventional Weapons (CCW). A breakthrough came at the end of 2016, when countries taking part in the treaty's five-year Review Conference agreed to formalise their deliberations on LAWS. The Conference established a Group of Governmental Experts (GGE), to be initially chaired by Ambassador Amandeep Gill of India. As of this writing, the GGE has held two sittings, in Nov 2017 and Apr 2018, with more to follow. Close to a hundred countries are participating in these meetings, along with representatives from UN agencies, the International Committee of the Red Cross, and the Campaign to Stop Killer Robots. In addition to the deliberations at the UN, discussions are also underway at several other forums world-wide, mostly at the behest of pro-ban advocacy groups. The views and counterviews being expressed on this emotive issue are multi-faceted and complex, which is why the progress towards consensus, including at the UN, is very slow.

This monograph is presented in two parts: in the first part, an endeavour is made to highlight several issues which are at the core of the ongoing debate and have come up in some form or the other over the last few years, but are perhaps

not getting discussed with sufficient analytical rigour. Special emphasis is laid on the importance of the military context against the backdrop of practical conflict scenarios, rather than providing broad-based arguments in the abstract, with the aim of achieving early convergence amongst opposing views.

The second part reviews the status of defence AI technology in India, assesses the current capability of the Indian Armed Forces to absorb this technology, and suggests steps which need to be taken on priority to ensure that we do not get left behind in the ongoing race by advanced militaries towards ushering in a new AI-triggered RMA.

LETHAL AUTONOMOUS WEAPON SYSTEMS: SLAVES, NOT MASTERS!

Views and Counterviews

Ever since the launch of the Campaign to Stop Killer Robots, a whole body of literature has emerged expressing a wide spectrum of opinion on LAWS. One of the first documents to initiate the debate was "*Losing Humanity: The Case Against Killer Robots*", issued by HRW/ International Human Rights Clinic (IHRC) in Nov 2012[1]. It enunciated its arguments based on the International Humanitarian Law (IHL) issues of *Distinction, Proportionality, Military Necessity* and the *Marten's Clause* as also the problems of *Accountability*. HRW/ IHRC followed this up with several other documents related to this subject, such as "*Shaking the Foundations: The Human Rights Implications of Killer Robots*" in 2014, focussing on the human rights angle, "*Mind the Gap: The Lack of Accountability for Killer Robots*" in 2015, which dwells on the accountability aspect of LAWS, and several others[2,3].

Ronald Arkin, one of the prominent authors arguing in favour of LAWS, makes a case for the development of *Ethical Robots,* and offers counterviews to the HRW position

in his piece "*Lethal Autonomous Systems and the Plight of the Non-Combatant*"[4] and a follow-up article "*Counterpoint*"[5], although he proposes proceeding with caution. Similarly, Michael N Schmitt argues strongly in support of LAWS in his incisive article "*Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics*"[6], in which he offers an issue-by-issue rebuttal of the arguments given out in IHRC's "*Losing Humanity*".

Other authors support the HRW case. Noel E Sharkey, in his article "*The Evitability of Autonomous Robot Warfare*"[7], disagrees with Arkin's views, essentially stating that Artificial Intelligence/ Autonomous Systems (AI/AS) would probably never be able to match up to the fantasy of creating *Ethical Robots* and meet the functional requirements of *Distinction* and *Proportionality*. He also suggests a five-level architecture for human supervisory control in another piece[8], which is a useful reference for taking forward the debate on MHC.

Regarding the feasibility of a ban on LAWS, Kenneth Anderson and Matthew C Waxman[9] argue that incremental development and deployment of autonomous weapons is inevitable, and any attempt at a global ban would be ineffective in stopping their use by the states whose acquisition of such weaponry would be most dangerous. They also assert that such weapon systems are not inherently unlawful or unethical. Peter Asaro[10] disagrees with this view, and goes further to state that pursuing the goal of *Ethical LAWS* is likely to degrade our conceptions and standards of ethical conduct, and distract us from developing the technological enhancement of human moral reasoning by chasing an improbable technology that threatens to undermine our human rights on a fundamental level.

Not surprisingly, there is not much available in the literature on AI/AS technologies per se which is likely to lead

to the development of "fully" autonomous weapon systems, not least because most of the technological breakthroughs necessary for their realisation are still in the realm of the future. Opinions, including those of leading AI/ robotics experts, vary widely. Ban proponents, of course, base their arguments on the premise that values such as "empathy" and "judgement" can never be simulated in machines. On the other hand, there are those who are convinced that Kurxweil's "Singularity"[11,12]would be achieved within this century, maybe sooner than later. There are also some futurists who are of the opinion that at a point in their development, LAWS will evolve sufficiently enough to possess "consciousness"!

A number of other authors have offered various perspectives on the complex issue of LAWS, and some of them have been referenced in context subsequently in this paper. The stand of individual governments on the issue of banning LAWS may be gleaned from their statements given at UNODA CCW LAWS meetings over the last four years. In summary, while a number of countries have expressed pro-ban views, none of the major players (US, Russia, UK, China, Israel, etc) appear to be presently leaning towards supporting such a ban and, going by their currently stated positions and actions, are not likely to do so in the future as well. The Campaign to Stop Killer Robots appears to be getting maximum impetus from human rights groups with HRW in the lead, renowned scientists and leading figures such as Stephen Hawking, Elon Musk, Mustafa Suleyman and Stephan Wozniak, as also players from the AI industry.

LAWS: Weapon Systems with a Difference

Existing UN Conventions banning weapons include the following: Biological (1975), CCW (1983; with individual protocols for mines, booby traps, incendiary weapons, blinding laser weapons and explosive remnants of war), Chemical

(1997), Anti-Personal Mines (1997) and Cluster Munitions (2010). The rationale for banning these weapons is based on the fact that they cause excessive injury, are indiscriminate, or are repugnant and "against the principles of humanity and the dictates of public conscience".

LAWS, as (loosely) defined in the ongoing discussions are, at a fundamental level, of a different flavour, for the following reasons:-

- The *weapon* itself (rifle, missile, artillery gun, tank, etc) is not the subject of debate, and in fact, is not even specified! It is the nature of the *weapon control system*, in particular the *algorithmic intelligence* which would lend *autonomy* to the weapon system, which gives rise to multiple concerns, triggering the debate on banning LAWS.

- Since autonomy is at the heart of the discussion on LAWS, understanding the employment of LAWS requires an in-depth understanding of the *complex interplay of machines and humans during the targeting process* in military operations, which is not a simplistic "aim and shoot" affair as many tend to believe.

- Unlike the "indiscriminateness" associated with chemical or biological weapons, where the nature of the weapon is such that their effects cannot be confined to combatants alone once unleashed, in the case of LAWS the "distinction" consideration emanates from the fact that the controlling algorithm *might not be intelligent enough to distinguish adequately* between combatants and civilians/ wounded/ combatants hors de combat, etc. This is based on the premise that LAWS cannot be designed to target a single or a group of clearly identified military target(s) (just like, e.g., a barrage of artillery fire), a presumption that may not be correct.

- Existing weapons may have a degree of inaccuracy and may not be perfectly reliable (as no system can be), but they are not characterised by *unpredictability*. The general perception of LAWS, on the other hand, is that they would be (possibly highly) unpredictable, and hence not under "human" control. Whether or not this notion is justified is discussed later in this work.

- There is a fear in some quarters that LAWS, if developed, would one day evolve to a stage where they would take over the human race. But much before that, even in their most basic avatar, *LAWS are visualised as being in competition with humans*. Probably stemming from the characteristics of *unpredictability* and *intelligence* associated with LAWS, this weapon system is visualised as having a mind of its own, including the power of "life or death" over humans. This has led to the coining of the "Killer Robots" slogan, and the view that deployment of LAWS impinges on human dignity and violates the Marten's Clause. In other words *an agency, and an amoral one at that, is implicitly associated with the idea of LAWS*! This aspect too will be discussed at greater length subsequently.

- In an apparently contradictory stance, the implicit (and factually correct) presumption that there is no moral agent (indeed, no agent of any kind) present within LAWS leads to *Accountability* issues.

Amongst weapons and weapon systems, therefore, LAWS can be said to be *a class apart*. As a result, for the GGE instituted by the CCW, while an understanding of IHL and international human rights law is essential, of equal import is a thorough understanding of complex, evolving AI/AS technologies, and an equally good grasp of military procedures, especially the targeting process, against the backdrop of a very wide spectrum of conflict.

LAWS: Terminology and Working Definition

Terminology

For the weapon systems under discussion, three terms currently in use are of relevance: Autonomous Weapon Systems (AWS), Lethal Autonomous Weapon Systems (LAWS) and fully (lethal) autonomous weapon systems (not ascribed with the acronym F(L)AWS!). There are some other terms, too, which one finds in the literature, such as semi-autonomous weapon systems, supervised autonomy, etc. It is felt that, since autonomy is a continuum as well as multi-faceted in nature (please see subsequent sections on autonomy), and it may not be possible to rigorously define "full autonomy", it may be best to restrict usage of terms to AWS and LAWS only, with the latter term defining that sub-class of AWS which could result in *human fatalities* (an anti-missile weapon system, for instance, would classify as an AWS but not come under the category of LAWS). The degree and facet of autonomy could then be expanded upon separately in the context of individual weapon systems.

Definition of AWS: Two Views

The following definitions reflect two different views in the ongoing debate:-

- The International Committee of the Red Cross (ICRC) has defined AWS as: "Any weapon system with autonomy in its critical functions. That is, a weapon system that can *select* (ie, search for or detect, identify, track, select) *and attack* (ie, use force against, neutralize, damage or destroy) targets *without human intervention*."
- As per ICRC, the advantage of this broad definition, which encompasses some existing weapon systems, is that it enables real-world consideration of weapons technology to assess what may make certain existing weapon systems acceptable – legally and ethically— and which emerging technology developments may

raise concerns under IHL and under the principles of humanity and the dictates of the public conscience[13].

- Although ICRC classifies their definition as "broad", an even broader definition proposed by Switzerland is also noteworthy. Switzerland describes AWS simply as "weapons systems that are capable of carrying out tasks governed by IHL in partial or full replacement of a human in the use of force, notably in the targeting cycle"[14].

- The contention of Switzerland is that such a working definition is inclusive, and allows for a debate that is differentiated, compliance-based, and *without prejudice to the question of appropriate regulatory response*. As per them, the working definition proposed by them is not conceived in any way to single out only those systems which could be seen as legally objectionable. At one end of the spectrum of systems falling within that working definition, States may find some subcategories to be entirely unproblematic, while at the other end of the spectrum, States may find other subcategories unacceptable.

It is evident that, of the two definitions, the one proposed by Switzerland is more inclusive. Their logic of not wanting to single out those systems which could be seen as objectionable, is also appealing. On the other hand, notwithstanding its claim of being broad in nature, the proposed ICRC definition, which also appears to be the popularly accepted de facto working definition in UNODA discussions, does appear to be aimed at targeting the problematic AWS, since it envisages no human intervention in the "critical" functions of "selection and targeting". It is also felt that Switzerland's definition seems to more accurately represent of what can be literally understood from the term "AWS".

IHL and the Critical "Select and Engage" Functions

In the ongoing debate, it is clear that autonomous functioning in the critical functions of "select and engage" triggers objections that such functioning is in violation to IHL principles of *Distinction*, *Proportionality* and the *Marten's Clause*[15]. A brief elaboration is as under:-

- Principle of Distinction. Ban proponents declare that machines will likely never be able to reliably distinguish between combatants (the intended targets) on the one hand and civilians, wounded combatants and combatants hors de combat on the other. Hence the "select to kill" function should never be delegated to them. Even in the case of combatants, it may be necessary to exercise *empathy* in certain scenarios, a characteristic which machines, having no moral agency, would *never* be able to possess.

- Principle of Proportionality. It is contended that adhering to the principle of proportionality requires *value judgement* taking into account a host of factors, and machines can *never* evolve to this level of human prowess. This is another reason put forth by ban proponents to advocate that "select to kill" decisions be never taken by LAWS.

- Marten's Clause. Ban proponents raise the ethical/philosophical issue of whether machines should ever be vested with the decision power of "life and death" with respect to humans (which is implicit in the "select" function) which, as per them, would be "against the principles of humanity and the dictates of public conscience".

Analysis

The following comments are offered in this regard:-

- First of all, it would be reasonable to accept the contention that, at least for the next couple of decades, LAWS will not evolve to the level of humans with respect to qualities such as moral and ethical behaviour, empathy and value judgement. Ongoing discussions on the need for prohibitory/ regulatory conventions should, therefore, be carried out under this assumption.

- However, making such an assumption does not automatically justify a ban on LAWS. This is because the spectrum of military conflict offers many scenarios where the principle of distinction is not applicable (this is not the same thing as saying that civilians are not present in the combat zone). Furthermore, proportionality judgements are generally made by a commander at a higher level of military hierarchy, while LAWS would be tasked with carrying out individual attacks at the execution level.

It is felt that *much of the difference in opposing views on the issue of LAWS being in violation of IHL can be resolved if discussions are carried out against the backdrop of a defined military context*, of which there is a very wide spectrum in 21st Century warfare. The next section makes such an attempt.

LAWS, IHL and the Spectrum of Conflict

Since we are familiar with drone warfare, let us look at a few not-so-futuristic scenarios of *autonomous* drone attacks in military operations.

Scenario 1: Mechanised Warfare

After declaration of hostilities, a commander tasks a swarm of armed drones to destroy maximum combat capability of an adversary tank formation located and known to be operating in a well-defined 100 square kms of desert terrain. The autonomous drone swarm is launched, carries out the mission

with a degree of success, and returns to base. In such a scenario, let us see whether IHL principles have been violated. Relevant aspects to consider are as under:-

- With current (pre-LAWS) capabilities, such a mission would be carried out by own forces using tank formations in conjunction with artillery and air support, including attack helicopters.
- Principle of Distinction. The "select" function in the drone swarm is restricted to identifying tank signatures in the designated area, selecting them one at a time and targeting them with on-board weapons. There are no civilians/ combatants hors de combat expected in such a combat zone, and even if they are, casualties amongst them would clearly be acceptable as collateral damage. *The 'distinction' capability is thus not needed in the autonomous drone swarm since, given the tactical setting, it would not be applied even by human soldiers in such a scenario*. It is also pertinent to mention here that the selection of the group target (which we may term as *group select*), in this case the group of enemy tanks, is carried out by a human commander before the autonomous drones are launched.
- Principle of Proportionality. Value judgement on *proportionality* and *military necessity* would be exercised by the commander at the time of *group select*, before launching the drone attack.
- Marten's Clause. The decision to destroy the group of tanks (with humans inside) is taken by the human commander. The task of the autonomous drones is merely to pick up tank signatures and destroy them one by one. This is pretty similar to the procedure which would be followed if the attack were to be carried out by manned aerial platforms. Thus, there appears to be no violation of the Marten's Clause.

Scenario 2: Attack on Logistics Infrastructure

A similar attack by autonomous armed drones can be visualised on logistics infrastructure in the adversary's hinterland in a hot war scenario, e.g., an ammunition dump, an airfield, a bridge or a group of such targets. *The difference here is that civilians would be present in and around the target area*. Civilians working within the ammunition dump would clearly be valid targets, while any civilian casualties on an attacked bridge would be acceptable as collateral damage. The assessment of military necessity would have been carried out by a human commander before launching the attack, just like in a similar strike carried out by manned aircraft.

Other Conventional Warfare Scenarios

Several other battle scenarios belonging to the conventional warfare sub-class of the spectrum of conflict may be envisaged, e.g., attack on a battalion defended area, attack on naval fleets, etc, all by autonomous armed weapon systems. The distinguishing features of all such attacks are that they are carried out on the declaration of hostilities between the adversaries, are restricted to designated combat zones or on well-defined military targets, and the selection of targets, individual or group, is carried out by a human commander *before* activating the LAWS.

Scenario 3: Counter-Terrorist Operations

In a politically turbulent peace-time situation, an autonomous armed drone attack is launched to destroy a group of terrorists known to have got together for a meeting at a particular venue (an "Eye in the Sky"[16] type of setting). The turn-around time from drone take-off time until return to base is several hours. The drone does not have the requisite sensors and intelligence to identify the terrorists from amongst the civilian population in the area. The chances of a change in situation from the time the attack was launched till the time it is carried out are high.

Analysis

Against the above backdrop, the following comments are relevant:-

- Do the drone attacks painted in Scenarios 1 & 2 and other conventional scenarios classify as "fully autonomous" as per the ICRC definition? Going by the flavour of the ongoing debate, the answer would be in the affirmative. Are the attacks objectionable to the proban proponents? If so, on what grounds?

- As per HRW, the conventional scenarios painted here are "narrowly defined constructs," framed merely to justify the use of LAWS[17]. In the opinion of the author, although in conventional warfare too there would be tactical situations where the use of fully autonomous weapon systems may not be warranted, the ones described here are the norm rather than the exception.

- On the other hand, under the presumption that LAWS have not yet evolved to possess the *distinction* capability, an attack such as the one described in Scenario 3 would violate existing provisions in IHL.

- It seems that the military contexts implicitly assumed by most participants are William Lind's Fourth Generation Warfare (4GW) scenarios[18] (post-Second Gulf War operations in Iraq, Operation Enduring Freedom in Afghanistan, ongoing operations against ISIS, etc.) which the world has been witnessing over the last decade and a half. Although such scenarios clearly need to be considered in the LAWS debate, it must be kept in mind that the capabilities of major world armies (US, Russia, China, India, etc.) are meant to fight conventional wars, notwithstanding the fact that the frequency of such wars has reduced significantly. *The acceptability*

or otherwise of LAWS for deployment in conventional war settings should, therefore, be the primary area of concern.

- Going by the above discussion it may be concluded that, in *typical conventional war tactical settings, LAWS are not likely to raise humanitarian concerns. On the other hand, in most 4GW scenarios, use of LAWS may not be acceptable at least in the foreseeable future.*

Autonomy vis-à-vis Human Control

Autonomy and Human Control are two facets of control which lie in a close relationship on opposite sides of the human-machine interface; where autonomy ends, human control begins. In a weapon system, this is a complex multi-functional relationship which, with the right balance, can achieve a powerful synergy. Further, while one can visualise a fully manual weapon system (e.g., a spear), a fully autonomous system may not be easy to conceptualise, as some level of human control over weapon systems is always likely to be there (unless the human race is taken over by machines!). Also, with progressive increase in autonomy in one or more functions associated with a given weapon system, the human-machine interface would shift in incremental steps to reflect this change.

The following sections take a deeper look at Autonomy and Human Control.

Autonomy: A Continuum

While autonomy may be discussed in a generic sense, here we are more concerned with autonomy as applicable to the "select and engage" functions in an AWS.

From the ongoing discussions it is clear that the term *autonomy* is not well-defined, and that clearly there are degrees of autonomy. Although the "Report of the 2016 Informal Meeting of Experts on LAWS" submitted by the Chairperson to

the Fifth Review Meeting in December 2016 states that "clear distinctions were made between tele-operated, automated and autonomous systems"[19], making such distinctions with clarity does not in fact appear to be feasible at all. Marra and Mcneil[20] have given an excellent exposition on autonomy in weapon systems, stating that "there is no bright line between automation and autonomy" and that "autonomy should be measured on a continuous scale."

A popular way to classify these degrees of autonomy uses the "human-in-the-loop", "human-on-the-loop" and "human-out-of-the-loop" clauses, the last representing full autonomy[21]. Noel Sharkey has extended this to a five-level classification for human supervisory control of weapons[22]. The US Department of Defence (DoD) in its Directive 3000.09 of 2012 uses the terms "semi-autonomous", "supervised autonomy" and "fully autonomous"[23]. Several other classifications defining different degrees and facets of autonomy exist in the literature, some of them at a more granular level[24,25].

Given that the requirement of human involvement in targeting decisions is at the core of the ongoing LAWS debate, none of the above types of classification adequately capture the different facets of human involvement which have relevance with respect to the targeting process. This issue is discussed in a subsequent section on Human Control.

It emerges, however, that *the degree of autonomy in weapon systems is a continuumwith multiple facets* (activate, navigate, identify, select, engage, assess), and any lines drawn to separate weapon systems into sub-classes based on this parameter are at best blurred. Also, *"fully autonomous" weapons are likely to defy a rigorous definition*, at least in the foreseeable future.

Autonomous Systems: Not Necessarily AI Powered

"Autonomy implies AI, which in turn implies unpredictability

leading to loss of human control, and hence there is a case for a prohibitory ban on LAWS!" This seems to sum up the tacit line of thinking of a good number of pro-ban participants in the LAWS debate. Here we examine the first part,i.e., whether the implementation of autonomy in LAWS, particularly in its "select and engage" functions, necessarily requires the use of AI concepts.

Let us take the example of the Harpy Suppression of Enemy Air Defences (SEAD) weapon system, which appears to meet all the parameters used today to define LAWS. Once launched, the Harpy looks for radar signatures by "navigating" to a designated area, "identifies" enemy radars by matching these against an on-board database of radar signatures, selects a "radar" (there may be more than one), and then dives down to "destroy" it using its explosive warhead[26]. It is also "lethal" and not purely anti-materiel (unlike the Phalanx close-in weapon system[27]), since a radar station is generally manned. Apparently it does not employ AI technology, or at least does not need to, given the nature of its operational capabilities. *There does not appear to be much of a hue and cry against the operational deployment of the Harpy, developed more than two decades ago, or for that matter against its more sophisticated successor, the Harop*[28]!

Close-in weapon systems such as the Phalanx too need not be AI-powered, as machine learning/ deep learning may not be essential for meeting such operational requirements. Of course the Phalanx, being anti-materiel and not lethal by design, would not fall under the classification of LAWS.

Thus, *autonomy does not necessarily imply an underlying AI technology*.

Are AI-Powered Systems Inherently "Unpredictable"?

One of the lines of argument often put forth by ban proponents in connection with the *Accountability* issue, is that LAWS

would be inherently unpredictable, being AI based with self-learning abilities. Since learning would be dependent on the external environment, every time the system learns and adapts, it would metamorphose into a "new system". This would have two implications: first, since its behaviour would keep on changing, it may not be feasible to keep it within defined parameters, thus making it's going out of human control a distinct possibility; and secondly, it would not be feasible to hold anyone accountable for its behaviour, in particular its "decision" to kill, on the grounds that designers and military commanders cannot be held responsible for something which is beyond their control.

Is the assumption that machine-learning, especially deep learning, would necessarily lead to unpredictable behaviour, justified? Here, we are primarily concerned with the "select" function, to ensure that only the intended military targets are selected and engaged. The "navigate" function is also relevant here, since it needs to be ensured that the LAWS do not operate out of a designated target area.

The year 2020 appears to be the target for market leaders (Ford, GM, Renault-Nissan, Daimler) for bringing self-driving cars with Level 4 Autonomy (cars that can drive themselves without any human intervention) to the roads[29]. A truly driverless car with Level 5 Autonomy (with no brakes or steering wheel) could not be very far away from becoming a reality. As per Elon Musk, "Almost all cars produced will be autonomous in ten years[30]." Although the relevant technologies are still under development, it is pretty clear at this stage itself that AI is a core technology which will enable these targets to be met. It is evident that "unpredictable" self-driving cars are not going to be commercialised and put on the roads. Therefore, there is a reasonable degree of confidence even today that supervised/ deep learning algorithms are expected to yield controlled behaviour, well within design parameters, *even in an*

unpredictable environment.

At the same time, Elon Musk has also endorsed the "Campaign to Ban Killer Robots", and has flagged AI as an existential threat to humanity, if left unregulated[31]. *In the context of LAWS, deep learning is likely to be utilised in both the "navigate" and "select" functions, and the end result can be expected to be as reliable and predictable as in self-driving cars*. Thus, in the typical conventional war scenarios discussed above, LAWS may be relied upon to distinguish and target well defined military targets in a combat zone bounded in area and time, but maybe not to accomplish the complex task of identifying a terrorist amongst a civilian group, or even to distinguish a civilian from a combatant, at least in the near future. In supporting the pro-ban advocacy groups, perhaps Elon Musk is merely trying to caution against the use of AI agents at operational and strategic levels of warfare, and not at the "select and engage" execution level.

The amazing success demonstrated by the AlphaGo program developed by Google's DeepMind in beating a 9-dan professional Go player in 2016[32] also demonstrates that *machine learning systems can be designed to achieve desired goals, even though the path to the goal may not be transparent to the developers in every case*.

Safeguarding Against Automating the "Will"

It has been discussed in the previous section that machines which use deep learning techniques have the characteristic of being able to continuously metamorphose into something for which they were not specifically designed, depending essentially on the environment in which they operate. This characteristic, together with the fact that, being too complex, such "evolution" is non-decipherable by their original designers, is the primary cause for rising consternation amongst AI professionals over designing LAWS.

It has also been brought out above that machine-learning systems can be designed such that their unpredictability is confined within acceptable limits. Going further, there is also the aspect of internal isolation amongst the different functions of a complex system. Thus, the activate/ navigate/ identify/ select/ engage/ assess sub-functions of LAWS, even if capable of self-learning individually, need not share a common "intelligent" hardware, unlike the human brain. In other words, given the current machine learning design methodologies, it should be perfectly feasible to physically isolate the self-learning mechanisms of sub-functions in such a manner that, while individually they might suffer from the much-feared *unpredictability*, the design could ensure that interaction amongst the sub-functions is under perfect algorithmic control, thus limiting their unpredictable behaviour to individual sub-functions.

Flowing from the above, while the critical "select" and "engage" sub-functions may separately rely on deep-learning techniques, as long as the implicit "decide" sub-function interposed between these two is under strict human/ algorithmic control, the LAWS cannot be said to possess an "autonomous will" which might make it run amok, as many imagine.

Human Control

Having discussed autonomy, a few noteworthy aspects of "human control" - the other facet of weapon control - are now highlighted. Some remarks are also made on the dividing line between autonomy and human control, i.e., the human-machine interface. However, at the outset it is worth remarking that, *since degree of autonomy is a continuum rather than a set of logical discrete stages, that too spanning multiple functions, human control also must necessarily possess similar characteristics since, as stated earlier, human control takes over where autonomy ends*.

MHC in Critical Functions

In the Final Report of the 2016 CCW Meeting of Experts, it was stated that "meaningful human control" and "appropriate level of human judgement" were two alternative frameworks proposed by the participants for taking forward the discussion on the degree of human control in LAWS[33]. As per HRW/ IHRC, in the arms arena, the term MHC signifies control over the selection and engagement of targets, that is, the "critical functions" of a weapon system. It goes on to assert that humans should exercise control over *individual attacks*, not simply overall operations[34].

"Life Cycle" of AWS

On human control, the ICRC is of the view that control may be exercised by human beings at different stages: *development* of the weapon system, including its programming; the *deployment* and use of the weapon system, including the decision by the commander or operator to use or activate the weapon system; and the *operation* of the weapon system during which it "selects and attacks" targets. It considers whether control in the first two stages is sufficient to justify minimal or no human control at the operation stage from a legal, ethical and military-operational standpoint. ICRC further opines that this may depend on various technical and operational parameters, such as task, type of target, time-frame of operation, potential for intervention, etc[35].

Key Elements of MHC

In a particularly insightful commentary on the key elements of MHC, Richard Moyes, in a background paper prepared for 2016 CCW Meeting on LAWS, states the following: -

- As per its existing provisions, IHL provides a framework that should be understood as "requiring human judgment and control over *individual attacks* as a unit

of legal management and tactical action". He goes on to elaborate that *an individual attack is not necessarily a single application of kinetic force to a single target object*. In practice, an attack may involve multiple kinetic events against multiple specific target objects. However, there has to be some spatial, temporal, or conceptual boundaries to an attack if the law is to function.

- He asserts that, for the law to function meaningfully, there needs to be legal judgment and accountability over actions at the most local (tactical) level, as expanding the meaning of "single attack" to mean an attack at the operational or strategic level may render the concept of human control meaningless.

- He also proposes the following as key elements for further discussions on defining MHC: predictable, reliable and transparent technology; accurate information for the user on the outcome sought, the technology, and the context of use; timely human judgement and action, and a potential for timely intervention; and finally, accountability to a certain standard[36].

The Multi-Level "Select" Function

It emerges from the above discussion that the critical "select" function may have multiple interpretations, depending on the scenario. In one situation, a single military target may be selected for engagement just before release of the actual lethal force. In another,a commander may select a group of military targets even before the LAWS is launched (please see conventional scenarios discussed above), and after navigating to the target area, the AWS selects an individual target (or several individual targets one at a time) from amongst the selected group and releases the lethal force to destroy it (each). In this case, the decision on taking human lives would have been taken at the time of "group select" by the human commander and not by

the AWS at the time of actual engagement, and therefore would not be in violation of the Marten's Clause. As has been pointed out earlier, discussions on MHC within a specified military context may be key to arriving at a common understanding on this complex issue.

The Human - Machine Interface

In order to emphasise the synergetic relationship between humans on the one hand and AWS on the other, the alternative viewpoint to MHC is that it is the human-machine interaction which needs to be optimized. As per this view, proposed by the US[37], the human-machine relationship extends throughout the development and employment of the AWS, and is not limited to the moment of decision to engage a target. Flowing from this logic, as per this view it would be more useful to talk about "appropriate levels of human judgement" rather than MHC.

Analysis

From the body of opinion which has emerged on the aspect of human control in the LAWS debate so far, the following may be summarised:-

- Although suitable other terminologies, such as "appropriate level of human judgement", may be arrived at to express the complex connotation of human control over AWS, MHC appears to the more popular and acceptable term so far.
- For ensuring adherence to existing provisions in IHL and human right law, as also matching up to morality and human dignity standards, MHC does not necessarily imply that each and every release of kinetic force be specifically approved by a human operator/ commander.
- *The critical "select" function has multiple interpretations*

which are context-specific, and autonomy in the "select and engage" functions at the execution stage does not necessarily imply that an implicit "decision to kill" has been taken by the AWS, thereby violating the spirit of Marten's Clause.

- A number of technical and operational parameters need to be considered before concluding whether or not the desired level of human control has been exercised. Thus there may a case for focusing on the human-machine interface, in order to reap the benefits of the best synergetic combination of humans and AWS.

It is suggested that further work in this area needs to concentrate on coming to a common understanding on the above aspects, as also identifying the key elements of human control on the lines discussed above.

Saving Lives

As already discussed, the arguments for banning LAWS are primarily based on the premise that they would violate the IHL principles of distinction and proportionality. Both of these principles are directed towards saving innocent civilian lives. Further, in these arguments, *LAWS are being compared with humans, and that too humans who are in situations where human qualities such as empathy and making value judgements (on proportionality aspects) are required to be exercised.*

As per an alternative perspective aimed at bringing out the positive value of LAWS, *there is perhaps a case to compare LAWS to "dumber" weapon systems such as artillery guns and "fire and forget" missiles*, and how the higher intelligence of LAWS can lead to lesser collateral damage.

Saving Combatant Lives

In conventional warfare, once hostilities are declared, more often than not humans operating traditional weapon

systems are not called upon to exercise any of these "human" capabilities. For a soldier defending his locality against an adversary offensive, every adversary combatant is a target. For combatants manning an artillery gun position, given a target the sole aim is to neutralise it with a barrage of fire using the calculated amount of kinetic explosive. Long range precision vectors ("fire and forget" missiles), once released, proceed to destroy their designated targets with no further consideration for civilian casualties. For a tank formation in mechanised warfare, all efforts are made to inflict maximum tank losses on the adversary while the battle is on. The singular task of Air Force fighter pilots is to bring down enemy aircraft or neutralise enemy logistics infrastructure in the hinterland with minimum losses to own air assets. If the soldier in defence, the artillery gun positions, the tank formations and the fighter/bomber aircrafts are made autonomous in functioning, there would be a huge saving in lives of *own combatant soldiers*.

Saving Civilian Lives

Precision munitions are preferred over "dumb" munitions, even from a humanitarian perspective, because their lethality is more precisely directed at military targets, as a consequence of their being more "intelligent" than their dumber counterparts. LAWS are fundamentally more intelligent than precision munitions, although cognitively (as yet) inferior to humans. Therefore, even in scenarios where civilians are present, use of LAWS in place of dumb or even precision munitions for destroying valid military targets (military headquarters, logistics infrastructure) is expected to result in lesser *collateral damage*.

Analysis

The following important points are being made here:-

- The above discussion on saving lives does not presume that LAWS have evolved to the stage of exhibiting the human qualities of empathy, value judgement, etc.

- In the conventional warfare scenarios depicted above, LAWS are envisaged to be deployed in situations where qualities such as empathy (linked to the principle of distinction) are not applicable. Moreover, qualities such as value judgement (linked to the principle of proportionality) are indeed being exercised, but at a higher level of military operation, where a human is still in the loop. This would be the case even if LAWS were not utilised for combat.

- In conventional warfare, such tactical settings represent the norm rather than the exception. This is in refutation of the HRW contention that narrowly constructed hypothetical cases in which fully autonomous weapons could lawfully be used, do not legitimise the weapons because they would likely be used more widely[38].

- *Deployment of LAWS in typical conventional war scenarios is expected to result in significant savings of own combatant lives and also minimize collateral damage to civilians*.

Non-Feasibility of a Pre-Emptive Ban

To begin with, a coalition of advocacy groups called the International Committee for Robot Arms Control worked to promote an international convention to prohibit the use of LAWS. The call for an international ban was raised to greater prominence when, in November 2012, HRW issued a report calling for a sweeping multilateral treaty that would ban outright the development, production, sale, deployment, or use of LAWS. Many other organisations and groups, including some states, have now joined in to demand an outright ban on the development of LAWS.

On the other side of the debate are those who hold the view that, *even if justified*, the implementation of such a ban

may not be feasible primarily due to the following reasons, amongst others:-

- Autonomous technologies will be implemented "incrementally" into military weapon systems on their march towards "full" autonomy, making it difficult to assess when the ban threshold is crossed.
- Dual-use technologies will, in any case, continue to be developed for civilian applications.
- It would be difficult to get high contracting parties at the UN to agree to sign such a convention, since there is no way to stop non-signatories as well as unprincipled signatories to march ahead in developing the requisite technologies despite the ban being in place.

In order to ensure a cautionary and controlled approach towards development of LAWS, nations have the option of putting into effect either a *prohibitory* or a *regulatory* convention. These are briefly discussed below.

Prohibitory Ban

On the issue of the workability or otherwise of a prohibitory ban, there are well-reasoned arguments given out in a research paper by Anderson and Waxman on the inadvisability of adopting such a course[39]. The following additional remarks need consideration:-

- There appears to be no objection from the ban proponents to the issue of autonomy per se, as long as there is a "man-in-the-loop."
- *A "decide" function is implicit in the conjoint "select and engage" functions, the so-called critical functions*. If an AWS selects a target autonomously, takes human approval for engagement, and then engages the target

again through an autonomous process, the "human-in-the-loop" criteria would clearly be satisfied.

- What needs to be taken note of here is that *it is for implementation of the "select" function ("identify" being implicit in "select") that sophisticated AI technologies are expected to be utilised*. AI facilitated technologies may also be utilised to improve the "navigate", "track", "engage" and "assess" functions in the targeting "kill chain". In contrast, *the "human approval based decide" function, which separates the "select" and the "engage" stages in a man-in-the-loop AWS, is pretty trivial in terms of technology*.

- The above implies that a ban convention signatory can go ahead and develop an acceptable "man-in-the-loop" AWS, with all kill-chain functions as sophisticated as needed for a fully autonomous weapon system. Thereafter, *the transition from this to a fully autonomous system would just be a trivial step*. This also implies that a ban on the development of technology is not likely to be effective.

- Another noteworthy aspect is as follows: all other weapons banned vide existing conventions – chemical and biological weapons, cluster munitions, mines, etc.—if used in a conflict—can easily be detected from their physical effects. On the other hand, even though extensive weapon reviews may have taken place at the development stage on a man-in-the-loop AWS, *whether or not it is functioning in a fully autonomous mode would never be evident from its characteristics in action!* In other words, *the trivial transition from a man-in-the-loop to a man-out-of-the-loop system would be almost impossible to verify*.

Regulatory Convention

On the one hand, due to reasons discussed above, there does not appear to be much hope towards putting a prohibitory ban in place, and even if achieved, may not have much meaning. On the other, *a regulatory convention on LAWS which restricts the deployment of LAWS to certain well-defined scenarios (such as the ones discussed in this paper), and/ or prohibits their use in another set of scenarios, and also puts together review mechanisms in place, may find success in achieving a high degree of consensus amongst the high contracting parties at the UN*. Having stated that, it is also pointed out here that militaries operate under the ambit of well-structured rules of engagement, and deploy weapon systems only in environments for which they are designed. *A regulatory convention, therefore, may well serve the purpose of satisfying the concerns of human rights advocacy groups, but is not likely to materially affect their usage in the field*.

Development of LAWS: The Debate Goes On

With the institution of the GGE, efforts to forge a consensus amongst the high contracting parties are expected to get more focussed with time. Discussions over the last four years have helped to generate a large body of opinion which, it appears, is characterised more by diversity of views rather than their convergence.

It would be interesting to follow the direction which is taken by the debate during the CCW GGE meetings later this year and subsequently, towards achieving a consensus amongst the high contracting parties at the UN on the issue of banning/ regulating LAWS.

AI IN MILITARY OPERATIONS: WAY FORWARD FOR THE INDIAN ARMED FORCES

The previous section has deliberated upon in detail on the arguments being put forward by parties on both sides of the ban-LAWS debate. Going by the progress made so far, the likelihood of such a ban fructifying in the foreseeable future is extremely bleak. Even if such a convention is adopted by the UN, given its adverse impact on military capabilities, major world powers are unlikely to be signatories to it. This is quite evident from the official statements made at the recent GGE meeting in Apr 2018 by the main stakeholders[40,41,42].

In such a scenario India, which has adopted a non-committal stance at the UN[43] and has made little efforts to develop LAWS so far, needs to come to grips with the situation which is unfolding on the global conflict landscape. This is because, by not taking up the development of LAWS on a war footing, it would be placing itself militarily in a vulnerable position in any future conflict.

This part of the monograph first reviews the status of development of LAWS by major world players. Thereafter, keeping in view the Indian security scenario, it discusses the military applications of AI in general and LAWS in particular, and suggests steps which may be taken at the national level as well as by the Indian Armed Forces to harness the power of AI in the military context.

AI: Harbinger of the Next RMA

To put things in perspective, Information and Communication Technologies (ICT) have resulted in the *current* Revolution in Military Affairs (RMA), altering the nature of 21st Century warfare in ways never imagined before, by spawning new concepts such as Network Centric Warfare[44] and Information Operations[45] including Cyber Warfare[46]. The ongoing drone

operations are a stark example of how this RMA has manifested itself on the canvas of global conflicts.

The use of AI and Robotics technologies in military applications is widely believed to be the harbinger of the *next* RMA[47], in the not too distant future. This is the reason why the US, Russia, China and other advanced militaries are pursuing development of these technologies from a national strategic perspective, and investing billions of dollars in this area. Since many AI/ robotics based weapon systems are not capital intensive in nature, these are bound to find their way into the inventory of terrorist organisations as well.

Unfortunately, India is only now taking baby steps towards harnessing AI technologies in general and AI-powered defence applications in particular. Perhaps as a result of being preoccupied with the huge challenges being faced on operational and logistic fronts including issues related to modernisation, the AI/ robotics/ LAWS paradigm is yet to become a key driving force in the doctrinal thinking and perspective planning of the Indian Armed Forces. The frenetic activity taking place the world over in this vital field dictates that this state of affairs needs to change.

Military Applications of AI

There is a wide spectrum of AI-powered military applications which may be envisaged, all of them relevant in the context of the Indian security scenario. These may be broadly classified into the following three areas:-

- **Knowledge Applications.** AI applications which analyse unstructuredas well as collated data to derive knowledge for decision support would fall in this category. Surveillance applications providing multi-sensor data fusion by utilising audio, image and video processing functions, are a good example of this category.

- **Cyberspace Operations**. AI based tools and weapons which power autonomous offensive and defensive cyberspace capabilities comprise this category.

- **Autonomous Robotic Systems.** This category would include any military system which exploits AI and robotics technologies to achieve some autonomous capability on the physical battlefield, not necessarily lethal. Having stated that, it may be noted that autonomous military systems do not necessarily have to be based on AI technologies. LAWS would be a sub-category of such systems. The motivation for introducing increasing autonomy in military systems is primarily to shield humans from risk on the battlefield, and secondarily to increase combat efficiency.

Since the focus of this work is the current debate on LAWS, further discussion would mostly be restricted to autonomous robotic systems.

Employment of Autonomous Military Systems

The Indian military landscape comprises of a wide variety of scenarios where autonomous systems, and more specifically LAWS, can be deployed to advantage. The categorisation given below divides the autonomous robotic military systems into further sub-classes. This classification, in addition to exhibiting an increasing degree of complexity, takes into consideration parameters which have relevance to the ongoing debate on LAWS[48], as explained below:-

- **Non-Lethal and Defensive**. Autonomous systems designed to disarm Improvised Explosive Devices (IEDs) are already in use, including by India, although existing systems may not have much AI content. Such systems are "non-lethal" and "defensive" in nature.

- **Non-Lethal and Offensive**. An AI-enabled swarm of

surveillance drones (as opposed to manually piloted Unmanned Aerial Vehicles (UAVs) or Unmanned Undersea Vehicles (USVs)) could greatly boost our surveillance capabilities. Such a system would be "non-lethal", in support of both offensive and defensive operations.

- **Lethal and Defensive**. Deployment of Robot Sentries along an International Border (IB) or any military front-line (such as the Line of Control (LoC) in the case of India), would be a typical example of this class of autonomous weapons, characterised by being "lethal" and "defensive" in nature.

- **Lethal and Offensive**. Remotely piloted armed UAVs in use today are essentially manually controlled. Deployment of armed UAVs/USVs with increasing degrees of autonomy in the navigate/ search/ detect/ evaluate/ track/ engage/ kill functions, is clearly on the horizon. Such systems may be classified as "lethal" and "offensive". At the next level of sophistication in this class, lethal or "killer" robots deployed in land-based conventional operations alongside human soldiers, however, would require the breaching of many daunting technological barriers, before they can become a reality on the battlefield.

- **Lethal, Offensive and Ethical**. If robot soldiers are to be successfully deployed in Counter-Insurgency (CI) or Counter-Terrorism (CT) operations, an even higher AI technology threshold would need to be crossed. This is because, in addition to possessing a more sophisticated "perceptual" ability capable of picking out an adversary from amongst a friendly population, qualities such as "empathy" and "ethical values" similar to humans would need to be imbibed into such systems. As per one school of thought, this capability can never

be achieved, while others project reaching such a technological "singularity" within this century.

The last three categories would fall within the definition of LAWS. Also, the distinction between "Lethal and Offensive" and "Lethal, Offensive and Ethical" has been deliberately made here, since it is felt that there are many battlefield scenarios where LAWS without the "Ethical" characteristic may be deployed without violating the laws of war. This aspect has already been discussed at length in the previous section. It also merits mention here that ban proponents are largely accommodative towards the employment of "lethal and defensive" systems, but not so for "lethal and offensive" systems, based on their conviction that the "ethical" requirement is essential in *every* military scenario, and that this cannot *ever* be achieved in a machine based AI agent.

Technologies needed for the first three categories of military systems have already been developed to a good degree of sophistication by several militaries. In India, however, the power of AI has hardly been exploited in defence applications, be it weapon systems, surveillance applications, decision support systems, big data analytics, etc. Existing robotic systems deployed for defusing landmines and other explosive devices have limited autonomy, and do not have a strong AI component. Therefore, we must take all the necessary steps on priority to develop such systems indigenously. Simultaneously, research into more challenging areas as characterised by the last two categories, must also be initiated.

AI in Military Operations: Global Perspective

LAWS: Current Status of Deployment

As of now, near-autonomous defensive systems have been deployed by several countries. The better known autonomous defensive weaponry are the anti-missile defence systems, such

as the Iron Dome of Israel and the Phalanx Close-In Weapon System used by the US Navy. South Korea uses the SGR-A1, a sentry robot with an automatic mode, in the Demilitarized Zone with North Korea. Offensive weapon systems, in contrast, are those which can proactively seek out targets. Fire-and-forget weapons, such as the Brimstone missile system[49] of the United Kingdom and the Harpy Air Defense Suppression System of Israel, are meant for use in an offensive role and are near-autonomous. Another example of an offensive autonomous system likely to be deployed in the near future is Norway's Joint Strike Missile, which can hunt, recognise and detect a target ship or land-based object without human intervention[50].

US AI Supremacy and the Third Offset Strategy

The US has put AI at the centre of its quest to maintain its military dominance. In November 2014, the then US Secretary of Defense Chuck Hagel announced a new Defense Innovation Initiative, also termed as the Third Offset Strategy. Secretary Hagel modelled his approach on the First Offset Strategy of the 1950s, in which the US countered the Soviet Union's conventional numerical superiority through the build-up of America's nuclear deterrent, and on the Second Offset Strategy of the 1970s, in which it shepherded the development of precision-guided munitions, stealth, and Intelligence, Surveillance, and Reconnaissance (ISR) systems to counter the numerical superiority and improving technical capability of Warsaw Pact forces[51,52,53].In 2015, the Pentagon's fiscal 2017 budget request included $12-15 billion to fund new technologies, including autonomous weapons and unmanned aircraft, drone mother ships and deep-learning machines. These investments, and the major role they reserve for AI in future military force projection, reflect the core logic of the Third Offset Strategy[54].

One of the best articulations of current US strategic thinking can probably be found in the 2016 study on Autonomy

by the DoD's Defense Science Board (DSB). The study focuses on "institutional and enterprise strategies to widen the use of autonomy; approaches to strengthening the operational pull for autonomous systems; and an approach to accelerate the advancement of the technology for autonomy applications and capabilities". The study concludes with the observations that advances in AI have ensured that autonomy has now crossed a 'tipping point' and recommends that the DoD "take immediate action to accelerate its exploitation of autonomy while also preparing to counter autonomy employed by adversaries[55].

Chinese Initiatives

As the second biggest player in general-purpose AI, China is increasingly demonstrating that it is not far behind the US in this field. Chinese military leaders and strategists believe that the nature of warfare is fundamentally changing due to unmanned platforms. China's leaders have labelled AI research as a national priority, and there appears to be a lot of co-ordination between civilian and military research in this field[56]. In February 2017, China's National Development and Reform Commission commissioned Baidu to set up a research effort which will focus on machine learning-based visual recognition, voice recognition and new types of human-machine interaction. Meanwhile, major Chinese companies such as Baidu, Alibaba and Tencent have achieved notable breakthroughs in fields such as speech recognition and self-driving cars.

This drive towards AI is the consequence of a growing synergy between private actors and civilian applications on the one hand, and government agencies, specifically the People's Liberation Army (PLA), on the other. In 2016, the Chinese government announced plans to develop a $15 billion AI market by 2018. These initiatives have been characterised as part of the "China Brain Plan", an ambitious effort to develop AI and deploy it for military supremacy and social governance.

Given that the PLA conventionally approaches military innovation through a lens of 'technology determines tactics', they may be more willing to relinquish 'meaningful human control' in favour of the advantages accruing out of AI powered military applications, including lethal systems[57].

Russia's Efforts

While still lagging behind its great power rivals in terms of deep machine learning capabilities, Russia has displayed a clear commitment to developing and deploying a wide range of robotic military platforms, with the full backing of its Ministry of Defence (MoD) and domestic industries. Last year, President Putin said that AI is "humanity's future" and that the country that masters it will "get to rule the world"[58]. The Russian government is increasingly funding various AI-related projects, many under the auspices of the MoD and its affiliated institutions and research centres. Russia's Foundation for Advanced Studies, which was created as a parallel to the US Defence Advanced Projects Research Agency (DARPA), has recently announced proposals to standardise AI development along four lines of effort: image recognition, speech recognition, control of autonomous military systems, and information support for weapons' life-cycle.

However, Russia's annual domestic investment in AI including by its private sector is only a fraction of the global total, and Western and Chinese efforts are currently well ahead of Russian initiatives in terms of funding, infrastructure, and practical results. Yet, the Russian government is clearly aiming to marshal its existing academic and industrial resources for R&D breakthroughs in AI[59].

Israel's Successes

Israel was one of the first countries to declare its deployment of fully automated robots: self-driving military vehicles to patrol

the border with the Gaza Strip. As the next step, the Israel Defence Forces plan to equip these vehicles with weapons, and deploy them on Israel's borders with Egypt, Jordan, Syria, and Lebanon. As brought out above, the Israeli 'Harpy' anti-radiation UAV is able to detect, target, and engage enemy radar installations without any human oversight or supervision. Various Israeli companies apply AI in a number of their defence systems. Israeli contractor Aeronautics Ltd has produced a range of UAV control systems which are said to be powered by AI algorithms. Israeli defence electronics company Elbit Systems Ltd produces a Command and Staff Trainer that simulates a range of joint operations. In the future, the IDF plans to form mixed combat units of robotic vehicles and human soldiers[60].

AI Initiatives by the Indian Government

Some welcome initiatives have been taken by the Government of India in recent months. In August 2017, the Ministry of Commerce and Industry constituted the "Task Force on Artificial Intelligence for India's Economic Transformation" under the chairmanship of Dr V Kamakoti of IIT Madras. The task force submitted its report in Mar 2018, recommending the establishment of a National AI Mission (N-AIM), enabling the setting up of data banks, setting standards, formulating policies, devising an AI Education Policy including re-skilling strategies, participating in international rule-making, and leveraging international expertise through bilateral cooperation. The report makes a mention of the applicability of AI technologies to national security, but this aspect does not receive a detailed treatment by the task force[61]. In another initiative, the Ministry of Electronics and IT has set up an internal expert committee in Oct 2017 to advise it on the policy for AI. The main focus of the Ministry is to strengthen cyber security with the use of AI[62].

In Feb 2018, the Ministry of Defence (Defence Production) set up a task force to prepare the country's future

AI roadmap for the development of both defensive and offensive warfare capabilities. The 17-member panel is led by Mr N Chandrasekharan, Chairman Tata Sons, has the National Cyber Security Coordinator Gulshan Rai as a member, and has representations from the Army, Navy, Air Force, M/s Bharat Electronics, Defence Research & Development Organisation (DRDO), Indian Space Research Organisation (ISRO), Atomic Energy Commission, selected IITs, the Finance Ministry, and a few business groups. The task force was required to submit its report within three months, which is awaited[63].

The Finance Minister, in his speech on the annual budget, indicated that the NITI Aayog will create a roadmap for the National AI effort. A committee has been formed under the Chairmanship of NITI Aayog Vice Chairman Rajiv Kumar to create this roadmap on research and development[64].

The above steps go to show that the importance of AI technologies for the progress of the Nation on all fronts, as also to keep pace with game-changing capabilities being developed by major world powers, has now been realised by the Government. However, having lost precious time on this front, and given our poor record on the development of cutting-edge technologies, it remains to be seen as to how vigorously these initial steps will be followed up in the coming years.

Track Record of DRDO

Chairman DRDO stated way back in 2013 that they are developing "robotic soldiers" and that these would be ready for deployment around 2023[65]. Given the DRDO's credibility based on past performance, such statements must be taken as an expression of intent rather than as the final word on delivery timelines. DRDO's main facility working in this area is the Centre for Artificial Intelligence and Robotics (CAIR), whose vision, mission and objectives all refer to the development of intelligent systems/ AI/ robotics technologies. DRDO has

achieved some headway in making a few prototype systems, such as the "Muntra" Unmanned Ground Vehicle (UGV) by the Central Vehicles R&D Establishment (CVRDE), "Daksh" remotely operated vehicle and the "Netra" UAV by the R&D Establishment (Engineers) (R&DE(E)), and several prototypes including robot sentry, mini mule, snake robot, wall climbing robot, etc, by CAIR. CAIR is also in the process of developing a Multi Agent Robotics Framework (MARF) for catering to a myriad of military applications. However, in order to keep in step with progress in the international arena, these efforts alone may not suffice[66,67,68,69].

CAIR, just like any other DRDO lab, is weakly structured to produce cutting edge defence technologies at par with the best in the world. DRDO establishments are not very successful in attracting the best human resource coming out of our premier institutions such as the IITs/ IISc. Their commitment to deliver top of the line products within acceptable time-frames also leaves much to be desired, due to lack of accountability to the end-user, i.e., the Defence Services.Thus, while there are islands of excellence within the DRDO/ CAIR and some good products developed by their laboratories have been successfully deployed by our armed forces, these are few in number and mostly fall short when measured against global benchmarks.

In the context of work being done by the recently instituted task force on military applications of AI, Secretary Defence Production Shri Ajay Kumar has stated that DRDO would be a major player in future AI based defence projects. *Given its poor track record, making DRDO central to our philosophy for development of LAWS and other AWS may not be advisable*[70].

Having said that, DRDO has two distinct advantages over other R&D options involvingthe Industry and Academia as main players: firstly, unlike the Industry, profits are not a constraining criterion; and secondly the DRDO community,

in a relative sense, possesses better domain knowledge about the armed forces. Thus, *with suitable organisational re-structuring to overcome the weaknesses brought out above, CAIR may be able to contribute usefully towards our national effort in this important area*.

Nonetheless, the primary model for developing LAWS needs to be more effective and powerful. The rest of this section attempts to outline the contours of such a model. Much of the discussion which follows is related to analysing the structural weaknesses of our existing Military-Industrial Complex (MIC) and recommending measures to address these weaknesses. The following analysis, therefore, is not confined to AI/ robotics based products alone, but to the complete spectrum of cutting edge defence technologies (amongst which AI/ robotics technologies happen to be of primary importance). However, linkages have been drawn as needed to our current discussion on military applications of AI in general and LAWS in particular.

Towards an Effective R&D Model for AI/ Robotics

The Draft Defence Production Policy 2018 (DPrP 2018) aims to "make India a global leader in … AI Technologies." Under its "Innovations and R&D" section, it states that a higher level mechanism will be put in place with involvement of Service organisations to identify capability voids in defining critical technologies to be developed. It mentions that the Services already have formal arrangements with top end technical institutions within the Country. It goes on to say that Centres of Excellence (CoEs) will be set-up with industry participation and active involvement of academia and R&D institutions[71].

While the objective of becoming a global leader in AI technologies may be lauded, it is necessary to analyse whether the mechanisms which are in place today, together with the additional steps proposed in the draft policy, are robust enough

to ensure that this lofty aim is indeed achieved. What is really needed is a strong synergy amongst the five main stakeholders: the Government, the Armed Forces, the DRDO/ PSUs, the Industry and the Academia.

Each of the above stakeholders have their strengths and weaknesses. The Government has the authority and finances, but lacks in-depth domain knowledge about the art of warfare as well as technology. The DRDO/ PSUs have moderately good technological expertise, possess limited domain knowledge about military affairs and are not accountable to the users. However, being captive to the MoD, they can afford to take on high risk projects. The Academia are best suited to carry out quality research and, if given the requisite support in terms of domain knowledge, the necessary resources and with a certain amount of re-structuring, promise the best potential for evolving cutting edge technologies and delivering working prototypes. However, they are not organised to meet the stringent standards of the Defence Services as far as environmental hardening and field trials are concerned. The top Industry houses also have access to quality human resource, albeit without the institutional expertise available with premier academic institutions for carrying out R&D in frontier technologies. Once the requisite technology is made available, however, they are well-structured to deliver usable end-products. At the same time, profit optimisation being their primary goal, they need to be provided sufficient incentives to take on high risk projects. Both the Academia as well as the Industry possesses very weak domain knowledge about military affairs.

Keeping in view all the above considerations, *the way forward for successfully indigenising defence products in the exciting new field of AI/ robotics must therefore emerge from a vibrant, synergetic interplay between the Industry and the Academia, with the Services at the fulcrum and the Government/ MoD in full support*.

Incentivising the Industry

India's overall investment in R&D is very low when compared to other countries. As per the 2018 Economic Survey Report, in 2015 India spent $48.1 billion on R&D, which was 0.8% of the GDP and the country has 156 researchers per million of the population.In contrast, the US invested $479 billion which was 2.8% of the GDP, and has 4,231 researchers per million of the population, while China spent $371 billion, which was 2% of its GDP, and has 1,113 researchers per million of the population. Israel's investment of $12.2 billion, while significantly less than India in absolute terms, was 4.8% of Israel's GDP. It outperformed India, USA and China in the number of researchers per million of the population, with the number at 8,255[72].

A related issue with Indian research is the disproportionate amount of money (over 60%) being spent on government R&D. A very high proportion of this goes to the DRDO, with not very encouraging results. In most countries producing state-of-the-art technologies, private investment into R&D far outstrips that by the government. *Indian manufacturers need to increase their investment into R&D, and in turn, need to be incentivised by the Government. The Defence Procurement Procedure 2016 (DPP 2016) has to some extent facilitated this process*.

In an important modification to the existing 'Make' Procedure, the DPP 2016 has divided 'Make' projects into two categories – Make-I (Government Funded) and Make-II (Industry Funded) – and has also provided extra incentives to the Micro, Small and Medium Enterprises (MSMEs). For Make-I projects, the Government provides funding up to 90% for prototype development by the industry; whereas for the latter category, which is largely confined to import substitution, the Industry is required to bear the full cost

of development. Also, in order to bring in a degree of accountability, the procedure provides for the mandatory issuance of the Request For Proposal (RFP) within two years of successful development, failing which the balance 10% funded by the Industry is also to be reimbursed to it. Successful prototypes developed under the 'Make' procedure would then be inducted under the Buy Indian Designed, Developed and Manufactured (IDDM) category, which is designated as the most favoured category for acquisition[73].

However, despite the 'Make' procedure being in vogue since DPP 2006 was issued, and the improvements to it effected in 2016, the Industry has not yet thrown up any defence technology breakthrough success stories. The reasons for this, therefore, need to be identified and remedied.

The Academia: Graduating from Consultants to Innovators

The 'Make' procedure is open only to Indian vendors registered for a minimum of five years (three years for MSMEs) and having a minimum credit rating of B++ from CRISIL/ ICRA, amongst other conditions. Academic and research institutions, therefore, are not eligible to participate under this or any other provisions of DPP 2016. A close scrutiny of DPP 2016 shows that the role of the Academia in the DPP is limited to providing advice, when co-opted on various committees/ panels. The underlying thought process appears to be that it is the Industry which must form R&D partnerships with the Academia, but the commercial interface for acquisitions with the MoD/ Services needs to be with the Industry.

This relegation of academic and research institutions (other than Government institutions such as the DRDO) to being a third party in technology development appears to be a fundamental flaw in the existing mechanisms to sponsor front-line research in complex fields, especially of the nature of AI/ robotics. At a juncture when new technological frontiers

in this field are being tackled and breached on the global stage, and in a situation where neither the Industry nor the Academia have even a rudimentary understanding of the Defence environment, such an arrangement is hardly likely to succeed. *Given the strengths and weaknesses of the various players involved as discussed above, it is felt that our premier technological/ research institutions perhaps hold the key to successful indigenous innovations in the field of AI/ robotics. However, the existing eco-system for Defence R&D does not appear conducive for effectively tapping their potential.*

The above scenario needs to be contrasted with, for instance, the methodology adopted by DARPA, which directly partners with academia for innovative research[74]. A sterling example of their approach towards harnessing the potential of the Academia is their Joint University Microelectronics Program (JUMP) venture[75]. In this model DARPA, along with a consortium of industry partners and several universities identified after thorough research, have come together to sponsor fundamental research in microelectronics technologies at the universities.

Worldwide, as the pace of discovery accelerates and global competition intensifies, universities are going in for entrepreneurship in a big way. As of 2017, more than 200 colleges and universities have launched centres dedicated for innovation or entrepreneurship as members of the Global Consortium of Entrepreneurship Centres. At a time when societal challenges are demanding discoveries involving expertise in diverse disciplines, fostering a culture of entrepreneurship is one of the most powerful ways that universities act as economic accelerators. At Carnegie Mellon, faculty and students started 173 new companies between 2011 and 2016, raising more than $1 billion in investments. About 74% of those funds remained in its home state Pennsylvania, contributing to the regional economy. Similar results can be observed in academic institutions across the US[76].

It is such a culture which needs to be spawned in Indian academic institutions as well, commencing with our premier institutions, for developing AI/ robotics and other technologies for defence as well as dual-use/ civilian applications.

In the Indian Army, a mechanism for sponsoring research on defence technologies already exists in the form of the Army Technology Board (ATB), which was earlier placed under HQ Army Training Command (ARTRAC), and has recently been brought under the wings of the Perspective Planning (PP) Directorate at Army Headquarters, with its activities now being coordinated by the Army Design Bureau (ADB). The ATB interacts directly with the IITs/ IISc, amongst other R&D agencies including the Industry, with the charter of developing new technologies and products required by the Army. However, the results achieved by the ATB ever since its inception have not been very enthusing, despite the eagerness often exhibited by the Academia to participate and deliver results in the service of the Nation.

One of the ways in which the tremendous research potential of our academic institutions may be effectively utilised is by creating technology innovation centres within the academic institutions, jointly funded by the Defence and the Industry, and with continuous active participation from both these partners, especially the Services.

At this juncture, we are in a situation where the DRDO's delivery on the R&D front has been far from satisfactory, the Industry does not feel motivated enough to allocate resources and participate in defence projects, and we have not been able to tap the tremendous potential of our premier academic institutions to contribute towards fulfilling our defence technology needs. *This leads to the suspicion that at least some of the reasons for these failures on multiple fronts in our efforts to harness defence technology might emanate from structural and*

functional deficiencies within the Defence Services. This aspect is discussed next.

The Services as Lead Sponsors of Defence Technology

The primary responsibility for ensuring our national security rests with the Defence Services. Hence, it is incumbent upon the Services to take all necessary measures for being fully prepared to fight the next war. In the context of achieving that combat edge through technological superiority, and in the light of shortcomings of external players discussed previously, this responsibility requires a thorough understanding of emerging technologies on the one hand and their impact on warfare on the other. This is especially true in the case of a nascent and complex field such as AI/ robotics, in a world where technological breakthroughs are occurring at a breath-taking pace.

As per DPP 2016 procedures, HQ Integrated Defence Services (HQ IDS) is required to prepare a15 years Long Term Integrated Perspective Plan (LTIPP), a five years Services Capital Acquisition Plan (SCAP) and an Annual Acquisition Plan (AAP). In addition, in order to share the future needs of the Indian Armed Forces with the Industry, it is required to bring out a Technology Perspective and Capability Roadmap (TPCR), covering details of the acquisition plans for a period of 15 years, for use by the Industry. This document, which is also required to specify preferred technologies desirable in the products being envisaged, is required to be made available on MoD website[77].

The latest TPCR 2018, which is required to guide the Industry till the late 2020s, comprises of 221 serials covering a whole spectrum of defence products listed under 19 different categories[78]. If our defence strategic planning was proceeding in tune with the developments on the world stage, one would have expected, in this TPCR, a separate section devoted to

AI/ robotics. A quick scrutiny of the serials shows that, let alone a separate section, the terms "artificial intelligence" and "robotics" do not figure at all, while the word "autonomous" occurs only once, that too in the context of an inertial navigation system. It may be safely inferred from here that *AI/robotics based autonomous systems have not yet seized the imagination of the Services. In other words, the important chain of events commencing with understanding technology, leading to new operational concepts, finally resulting in a long-term forecast of defence products, has failed so far in the context of AI/robotics/ autonomous weapon systems*.

The role of the Defence Services, in fact, extends well beyond defence technology forecasting. For *basic research* in the case of dual-use technologies, the necessary push for accelerating research efforts might come from the Industry, but certainly needs to be augmented, if not led, by the Defence Services. If the technology is not dual-use, however, the entire support for basic research would need to come from the Services. This is equally true for *all cases of applied research* for defence products.

The above support is not limited to financial/ infrastructure support alone. Given the almost total lack of domain knowledge about warfare with the Industry and Academia, a very close relationship needs to exist amongst defence specialists on the one hand and R&D personnel on the other, in order that the research may be guided in the right direction. Such a relationship can only be maintained by specialists in uniform who can speak the language of the scientists, since the reverse, ie, scientists understanding the art of warfare, is very unlikely, especially in the Indian context.

The important role of technical specialists in the defence forces towards successful harnessing of cutting-edge technologies cannot be over-emphasised. This role commences with the identification of potentially useful technologies, and extends across all stages of R&D

till the successful fielding of defence products, and even beyond. This is especially so for complex technologies such as AI/ robotics. However, the requirement of high levels of specialisation may not be as applicable to, for instance, the development of a Main Battle Tank (MBT), where ensuring the requisite technical qualifications of defence project managers may not present as much of a challenge.

21st Century Warfare: Need for Greater Agility

As has been brought out above, understanding of emerging technologies with possible defence usage is only the first step towards the development of high technology defence products. Even before significant R&D in the field of AI/ robotics can be undertaken, the operational need for the same must be established. As has been stated above, even as the prospect of an AI driven RMA looms on the horizon, the Defence Forces have not yet realised the full import of developing critical AI applications and systems. Had this not been the case, by now concept papers and doctrinal literature on how AI is expected to transform future warfare, and its implications for the Indian security scenario, should have emerged. This has not happened.

Despite being a thoroughly professional and committed force, perhaps because of our extended conventional borders and our deep involvement in counter-insurgency operations, our doctrinal thought has not kept pace with the changing nature of warfare in the 21st Century, and is still based fundamentally on the concepts of industrial age warfare, relying on brute force and physical destruction to achieve military success. Many evidences may be quoted in support of this contention. Our forces are far from the objective of achieving net-centricity, with very poor headway made in the fielding of our Tactical C3I and Strategic C4ISR systems, which have been under development for almost three decades now. The gradual shift of global conflicts into the Information Realm has ushered in the critical dimension of

cyberwarfare, which is another area we have not been able to address with the requisite urgency. Even doctrinal direction in the areas of Network Centric Warfare (NCW) and Information Operations (IO) is minimal. And now, our inability so far to determinedly move forward towards harnessing the power of AI/ robotics for military applications, is another reflection of our lack of agility in transforming ourselves in step with the fast changing nature of warfare in current times.

This is not to say that sophisticated industrial age warfare capabilities in terms of personal weapons, artillery guns, tanks, aircraft, ships and submarines are not a priority for procurement. Indeed, the procurement issues that loom large today are the lack of ammunition to fight a long drawn out war, our inability to induct the basic infantry personal weapons despite decades of effort, the long delayed MBT project, and so on. This is perhaps another reason why there has been insufficient focus on information age technologies driving the current RMA, and almost no focus on the AI technologies which are the harbinger of the next RMA.

The challenge today for the Indian Armed Forces, therefore, is to provision and maintain the best of conventional military capabilities and at the same time usher in and master 21st Century warfare doctrines and capabilities in sync with advanced world militaries. The first step in this direction must necessarily be the evolution of concepts and military doctrine. Thereafter, the Services must take the lead and become the primary driving force for carrying out successful indigenous R&D in critical fields such as AI/ robotics and autonomous systems.

Structural Reorganisation: Specialisation is the Key

The important role that defence technology specialists need to play for successful R&Din frontier technologies has been highlighted above. *As per DPP 2016, the entire technical management of projects has been delegated to the Service*

Headquarters (SHQ), while the MoD gets involved in the grant of Acceptance of Necessity and commercial negotiations beyond delegation limits specified for the Services. The DPP also directs each SHQ to establish a permanent Make-Project Management Unit (PMU), headed by a two-star rank officer and staffed appropriately with professionals of various specialisations. It further states that the Make-PMU Head will have tenure of three years and the staff positioned in PMU shall have longer tenures to ensure continuity during execution of projects. It goes on to say that Make-PMUs may also hire expert practitioners from domains such as finance, legal and technology, from public and private sectors[79].

Establishments and Project Management Offices (PMOs) to steer defence projects have been in existence in the Services for several decades. For instance, in the Indian Army the Directorate General of Information Systems (DGIS), together with a number of PMOs/ establishments (CIDSS, ACCCS, BSS, ASDC, MISO, etc) under its jurisdiction, is responsible for the development of all tactical and strategic information systems. In addition, we have PMO Tactical Communication System (TCS, erstwhile Plan AREN), which has been in existence for a long time for induction of tactical communications systems, and PMO SURAJ for EW systems. Other such establishments also exist. All of these work in conjunction with the DRDO, the Industry and to an extent the Academia for the development of new products. *The effectiveness of these organisations in steering defence R&D and acquisition of state-of-art defence technology leaves much to be desired, mostly as a consequence of structural deficiencies*.

Only a small percentage of officers posted to these organisations have the necessary academic qualifications and experience to handle their respective assignments. In contrast to the guidelines laid down in DPP 2016 for Make-PMUs, most tenures at functional level are of three years duration or less.

The establishments are not suitably structured to interact with the Industry and Academia across the country to the extent desirable. *Most importantly, many of the establishments listed above lack a sense of ownership, notably the DGIS, consequent to the fact that they are structured as all-arms organisations manned by officers on a single tenure basis, or in other words, a floating population of non-specialists. Nothing could be structurally worse from the point of view of developing cutting-edge defence technology*.

The above organisational structure is in sharp contrast to, for example, the structure of the US Army Research, Development and Engineering Command (US Army RDECOM). Just one of its six research centres, the Communications-Electronics RDE Centre (CERDEC), has on its rolls 1620 scientists, more than 100 of whom hold doctoral degrees, and over 40 uniformed personnel[80]; another, the Army Research Laboratory (ARL) has 2500 scientists with over 500 doctorates[81] and so on. The other Service components of the US DoD also have internal R&D set-ups. Additionally, DARPA provides superlative R&D support to the entire DoD. Clearly, there is a lot which can be emulated by our Defence Services from military technology giants in the realm of organisational structuring for defence R&D. Perhaps the only Indian defence establishment which can be said to have a 'specialist' focus is the Indian Navy's Weapons and Electronics Systems Engineering Establishment (WESEE), which is why it has a better track record of R&D successes compared to its peers elsewhere.

At the core of the structural weaknesses described above is the failure so far of our military leadership to appreciate the new frontiers being breached in the fields of AI/ robotics, and the expected impact of these technologies on 21st Century warfighting techniques. The MoD, too, has a huge role to play towards bringing in transformational changes to Defence R&D structure, but for this to happen a concerted effort is required to be made by HQ IDS/ the Services to come up with feasible

solutions and prod the MoD into taking the desired decisions. *Having acquired excellence over the years in fighting Industrial Age wars as also in carrying out CI operations, the Services must now focus their attention on 21st Century conflicts, wherein technological sophistication in its military systems and a culture of specialisation with regard to its human resource, supported by an accountable R&D ecosystem under its direct control, may be key to achieving the military stature which India strives for as an emerging world power.*

Way Forward for the Indian Armed Forces

The first step for the Indian Armed Forces is to develop concepts and doctrines for AI applications in defence at the Joint Services as well as individual Services levels. As a precursor to this, the Services should fix ownership and designate CoE for the highly specialist AI and Robotics fields. AI has its roots in computer science disciplines. In the case of the Indian Army (IA), computer sciences are the forte of the Corps of Signals, which is thus ideally suited to be the lead agency for AI, with the Military College of Telecommunication Engineering (MCTE) as the primary CoE. Robotics, on the other hand, has a prominent mechanical engineering bias, and thus falls under the purview of the Corps of EME. The Military College of Electrical and Mechanical Engineers (MCEME) is already a declared CoE for robotics. In the context of LAWS, which involve multi-disciplinary expertise in the fields of AI, robotics and communications, MCTE is best suited to be the lead agency. Concepts and doctrine with respect to the role of AI in future warfare come under the charter of HQ ARTRAC, which should develop these utilising expertise available with the CoEs subordinate to it. Similar solutions may be identified for the Indian Navy (IN) and Indian Air Force (IAF).

MCTE should be tasked to conduct short courses on AI for all arms officers, and include AI as a separate course

in its graduate and post-graduate programs. Also, our premier institutes (IITs, IISc) should be approached to conduct post-graduate programs in AI and Robotics, or have courses in these disciplines included in their computer science programs, which must then be attended by officers from the Signals and EME respectively.

As a follow up to the recommendations of the AI Task Force, an initial set of AI-powered pilot projects with medium-term development times (two to five years) and high operational benefits must be identified and initiated on priority. Tie-ups should be arranged with IITs/ IISc to establish project specific innovation centres with the help of industry partners, formally identified under DPP 2016 Make-I procedures. Concurrently, CARE, CVRDE and other DRDO laboratories may also undertake the same projects depending on their respective competencies. A PMO should be established by each Service, staffed by specialists in AI and robotics as well as domain experts related to the projects. All project managers must be given tenures for the life cycle of the projects. The PMO should be headed by a two-star ranked specialist officer, and should report to the respective operations directorates at SHQ.

All the measures listed above are recommended to be taken up in mission mode and completed in a maximum of two years. The results of these efforts should bear fruit as and when working prototypes (some of which may be purely software based) are demonstrated. Projects not making acceptable headway should be foreclosed mid-course. Extending a project beyond five years should only be done under exceptional circumstances.

Successful fielding of such AI/ robotics based high-technology projects will help in etching the contours of a strong Indian MIC, which presently is not a vibrant enterprise despite all the requisite resources being available to us.

In the longer term, as part of a major re-structuring, all defence R&D establishments presently organised under the DRDO are recommended to be placed under the control of the Services. Ideally, Service specific R&D establishments need to be created, through a major increase in R&D resources. We also need to find ways for getting the Industry and Academia to participate in a major way in defence ventures. It is evident that these steps can only be implemented by the Government. However, it is incumbent upon the Services to formulate feasible re-structuring solutions after thorough analysis, and then vigorously pursue them with the MoD.

It is felt that transformational thinking within the Services as well as at the national apex level is an absolute must for our Armed Forces to remain relevant in the information and AI driven future warfare scenarios. With this conviction, this section has suggested some measures which are within the jurisdiction of the Services and can be implemented with immediate effect. Also, a brief insight is given into how a more comprehensive and effective solution might look for rejuvenating our weak MIC, through major organisational restructuring. However, for this to pan out, deliberations at the highest levels are necessary.

CONCLUSION

This monograph has attempted to contribute to the ongoing debate on banning of LAWS by presenting contrarian world views and analysing them, with special focus on the military perspective. It is evident from the flavour of this monograph that it does not support the idea of imposing an outright ban on LAWS. At the same time, it is felt that genuine concerns of the pro-ban advocacy groups need to be addressed. Towards this end, this work has tried to highlight that a better understanding of AI-AS technologies on the one hand, and military procedures especially against the backdrop of a very

wide spectrum of conflict on the other, will go a long way towards forging a common view. It has attempted to offer some new perspectives, and highlighted existing ones which do not appear to have received the attention they deserve.

Given the complexity of the subject, it is felt that an in-depth rather than superficial treatment of various issues involved characterised by greater rigour in terminology, definitions and rationale, set up against well-defined military contexts, rather than generic assertions against an abstract backdrop is likely to yield faster results.

Since consensus on imposing a ban is not likely to be achieved anytime in the near future, and resting in the conviction that applications of AI/ robotics on the battlefield are going to revolutionise the nature of warfare in the not so distant future, the monograph goes on to analyse the approach which India should consider for harnessing these exciting new technologies for enhancing its military potential and comprehensive national power.

Notwithstanding the world-wide concern on development of LAWS from legal and ethical points of view, it is increasingly clear that, no matter what conventions are adopted by the UN, R&D by major players in this area is likely to proceed unhindered. Given our own security landscape, adoption of AI based systems with increasing degrees of autonomy in various operational scenarios is expected to yield tremendous benefits in the coming years. Perhaps there is a need to adopt a radically different approach for facilitating the development of AI-based autonomous systems, utilising the best available expertise within the country, ie, with the Industry, the Academia and the DRDO/ PSUs. The contours of such an approach have been outlined which, in addition to an action plan at the national level, entails a transformation in mind-sets and organisations within the Armed Forces as well. As it is with any

transformation, this is no easy task. Only a determined effort, with specialists on board and due impetus being given from the national apex level, is likely to yield the desired results.

Endnotes

1 International Human Rights Clinic, *Losing Humanity - The Case Against Killer Robots*, Human Rights Watch, Harvard Law School, Nov 2012, ISBN: 1-56432-964-X.

2 International Human Rights Clinic, *Shaking the Foundations: The Human Rights Implications of Killer Robots*, HRW, Harvard Law School, 2014, ISBN: 978-1-62313-1333.

3 International Human Rights Clinic, *Mind the Gap: The Lack of Accountability for Killer Robots*, Human Rights Watch, Harvard Law School, 2015, ISBN: 978-1-6231-32408.

4 Ronald Arkin, *Lethal Autonomous Systems and the Plight of the Non-Combatant*, AISB Quarterly, Jul 2013, pp. 1-9.

5 Ronald Arkin, *Counterpoint*, Communications of the ACM, December 2015.

6 Michael N Schmitt, *Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics*, Harvard National Security Journal Features, 2013, pp. 1-37.

7 Noel E Sharkey, *The Evitability of Autonomous Robot Warfare*, International Review of the Red Cross, Volume 94, Issue 886, June 2012, pp. 787-799.

8 Noel E Sharkey, *Towards a Principle for the Human Supervisory Control of Robot Weapons*, Politica & Società, Number 2, May-August 2014, pp. 11-12.

9 Kenneth Anderson and Matthew C Waxman, *Law and Ethics for Autonomous Weapon Systems*, American University Washington College of Law Research Paper No. 2013-11, Stanford University, The Hoover Institution, Apr 2013, pp. 7.

10 Peter Asaro, *On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision Making*, International Review of the Red Cross, Volume 94, Issue 886, June 2012,

pp 687-709.

11 Ray Kurzweil, *The Singularity is Near: When Humans Transcend Biology*, Pub. Penguin, Sep 2006, ISBN 978-0-114-303788-0.

12 *The Singularity is Near*, https://en.wikipedia.org/wiki/The_Singularity_Is_Near, accessed 18 Jun 2018.

13 *Views of the ICRC on Autonomous Weapon Systems*, CCW Meeting of Experts on LAWS, Geneva, 11-15 Apr 2016, pp.1.

14 Wollenmann Reto, *A Purpose-Oriented Working Definition for Autonomous Weapons Systems*, CCW Meeting of Experts on LAWS, Geneva, 11-15 Apr 2016, pp.1.

15 Ibid. 1, pp. 30-36.

16 *Eye in the Sky*, English Movie, Entertainment One Production Company, 2015, https://bleeckerstreetmedia.com/eyeinthesky, accessed 17 Jun 2018..

17 International Human Rights Clinic, *Making the Case: The Dangers of Killer Robots and the Need for a Pre-emptive Ban*, Human Rights Watch, Harvard Law School, Dec 2016, pp. 7, ISBN: 978-1-6231-34310, pp. 9.

18 William S Lind et al, *The Changing Face of War: Into the Fourth Generation*, Marine Corps Gazette, Oct 1989, pp. 22-26.

19 Chairperson of the Informal Meeting of Experts, *Report of the 2016 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS)*, Geneva, Dec 2016, pp. 4-5.

20 William C Marra & Sonia K McNeil, *Understanding the Loop: Regulating the Next Generation of War Machines*, Harvard Journal of Law and Public Policy, Vol. 36, No 3, 2013, pp. 22-23.

21 Christof Heyns, *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions*, UN General Assembly, Apr 2013, pp. 8.

22 Ibid. 8.

23 Ashton B Carter, *Autonomy in Weapon Systems*, US Depart of Defence Directive 3000.09, 21 Nov 2012, pp. 3.

24 Ibid. 20, pp. 22-25.

25 *Unmanned Aircraft Systems*, Joint Doctrine Publication 0-30.2, UK

Ministry of Defence, Aug 2017, pp. 13.

26 *Harpy*, Israel Aerospace Industries, http://www.israeli-weapons.com/weapons/aircraft/-uav/harpy/HARPY.html, accessed 17 Jun 2018.

27 *Phalanx CIWS*, Wikipedia, https://en.wikipedia.org/wiki/Phalanx_CIWS, accessed 17 Jun 2018.

28 *Harop Loitering Munitions UCAV System*, Airforce Technology, https://www.airforce-technology.com/projects/haroploiteringmuniti, accessed 17 Jun 2018.

29 *Path to Autonomy: Self-Driving Car Levels 0 to 5 Explained*, Car and Driver, Oct 2017, https://www.caranddriver.com/features/path-to-autonomy-self-driving-car-levels-0-to-5-explained-feature, accessed 17 Jun 2018.

30 Tom Ward, *Elon Musk: "Almost All Cars Produced Will Be Autonomous in 10 Years"*, Futurism, 17 Jul 2017, https://futurism.com/elon-musk-almost-all-cars-produced-will-be-autonomous-in-10-years/, accessed 17 Jun 18.

31 Samuel Gibbs, *Elon Musk: Regulate AI to combat 'existential threat' before it's too late*, The Guardian, 17 Jul 2017, https://www.theguardian.com/technology/2017/jul/17/elon-musk-regulation-ai-combat-existential-threat-tesla-spacex-ceo, accessed 17 Jun 2018.

32 *AlphaGo versus Lee Sedol*, Wikipedia, https://en.wikipedia.org/wiki/AlphaGo_versus_Lee_Sedol, accessed 17 Jun 2018.

33 Ibid. 19, pp. 7.

34 International Human Rights Clinic, *Killer Robots and the Concept of Meaningful Human Control*, Human Rights Watch, Memorandum to CCW Delegates, April 2016, pp. 1-2.

35 *Views of the International Committee of the Red Cross (ICRC) on Autonomous Weapon Systems*, CCW Meeting of Experts on LAWS, Apr 2016, pp. 3.

36 Richard Moyes, *Key Elements of Meaningful Human Control*, Article36, Background Paper for the CCW Meeting of Experts on LAWS, Apr 2016, pp.1-3.

37 Michael W Meier, *US Delegation Opening Statement*, UN CCW Informal Meeting on LAWS, Geneva, 11 Apr 2016, pp. 2.

38 Ibid. 17.

39 Kenneth Anderson and Matthew C Waxman, *Law and Ethics for Autonomous Weapon Systems*, American University Washington College of Law Research Paper No. 2013-11, Stanford University, The Hoover Institution, Apr 2013, pp. 20-21.

40 *Humanitarian Benefits of Emerging Technologies in the Area of LAWS*, Paper presented by the US at UN CCW/GGE Meeting on LAWS, Geneva, 9-13 Apr 2018.

41 *Position Paper*, submitted by China at UN CCW/GGE Meeting on LAWS, Geneva, 9-13 Apr 2018.

42 *Russia's Approaches to the Elaboration of a Working Definition and Basic Functions of LAWS in the Context of the Purposes and Objectives of the Convention*, Paper presented by Russia at UN CCW/GGE Meeting on LAWS, Geneva, 9-13 Apr 2018.

43 Bedavyasa Mohanty, *Command and Control: India's Place in the Lethal Autonomous Weapons Regime*, ORF Issue Brief, May 2016, pp. 05.

44 Lt Gen (Dr) R S Panwar, *NCW: Concepts and Challenges*, The Army War College Journal, Winter 2015.

45 Lt Gen (Dr) R S Panwar, *Information Operations: Concepts and Way Forward*, The Army War College Journal, Summer2016.

46 Lt Gen (Dr) R S Panwar, *Cyberspace: The Fifth Dimension of Warfare*, Future Wars, Jan 2018, http://futurewars.rspanwar.net/cyberspace-the-fifth-dimension-of-warfare-part-i/.

47 Lt Gen (Dr) R S Panwar, *Artificial Intelligence in Military Operations: Technology and Ethics - An Indian Perspective*, Strategic Yearbook 2018, United Services Institution, New Delhi, pub. Vij Books, Jun 2018.

48 Lt Gen (Dr) R S Panwar et al, *International Perspectives: Autonomy and Counter-Autonomy in Military Operations*, Panel Discussion, http://carnegieendowment.org, Carnegie Endowment for International Peace, Washington, 31 Oct 2016.

49 Nicholas Marsh, *Defining the Scope of Autonomy*, Policy Brief, Peace Research Institute Oslo, Feb 2014, pp. 2-3.

50 R Shashank Reddy, *India and the Challenge of Autonomous Weapons*, Carnegie Endowment for International Peace, Jun 2016, pp. 4.

51 Chuck Hagel, *The Defence Information Initiative*, Memorandum Sec of Def, 15 Nov 2014.

52 Peter Dombrowski, *America's Third Offset Strategy*, Policy Report, S Rajaratnam School of International Studies, Jun 2015, pp. 4.

53 Franz-Stefan Gady, *New US Defense Budget: $18 Billion for Third Offset Strategy,* http://thediplomat.com, posted 10 Feb 2016, https://thediplomat.com/2016/02/new-us-defense-budget-18-billion-for-third-offset-strategy/, accessed 18 Jun 2018.

54 *Artificial Intelligence and the Future of Defence*, The Hague Centre for Strategic Studies, The Netherlands, ISBN/EAN: 978-94-92102-54-6, 2017, pp. 83-87.

55 *Summer Study on Autonomy*, Report of the Defense Science Board, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, Jun 2016, pp. i.

56 Jonathan Ray et al, *China's Industrial and Military Robotics Development*, Centre for Intelligence Research and Analysis, October 2016, pp. 9-13.

57 Ibid. 54, pp. 77-80.

58 Samuel Bendett, *In AI, Russia is Hustling to Catch Up*, Defence One, 04 Apr 2018, https://www.defenseone.com/ideas/2018/04/russia-races-forward-ai-development/147178, accessed 06 Jun 2018.

59 Ibid. 54, pp. 81-83.

60 Ibid. 54, pp. 80-81.

61 Dr V Kamakoti et al, *The AI Task Force Report*, Ministry of Commerce and Industry, Government of India, New Delhi, Mar 2018, pp. 46-50.

62 Surabhi Agarwal, *IT Ministry Sets Up Panels for AI Roadmap*, The Economic Times, 10 Feb 2018, https://economictimes.indiatimes.com/news/politics-and-nation/it-ministry-sets-up-panels-for-artificial-intelligence-roadmap/articleshow/62858282, accessed 19 Jun 2018.

63 Sanjib Baruah, *AI to Enhance Armed Forces Strike Power*, Deccan Chronicle, New Delhi, 21 May 2018, https://www.pressreader.com/india/deccan-chronicle/20180521/281522226745986, accessed 06 Jun 2018.

64 Pranav Mukul, *Task Force Set Up to Study AI Applications in Military*,

The Indian Express, New Delhi, http://indianexpress.com/article/technology/tech-news-technology/task-force-set-up-to-study-ai-application-in-military-5049568, accessed on 06 Jun 2018.

65 Ibid. 50, pp. 11.

66 *Robotics Products*, Combat Vehicles R&D Establishment, DRDO Website, http://www.drdo.gov.in/drdo/labs/CVRDE/English/index.jsp?pg=Products.jsp, pp. 3.

67 *Robotics Products*, R&D Establishment (Engg), DRDO Website, https://www.drdo.gov.in/drdo/labs1/RDE(E)/English/indexnew.jsp?pg=products.jsp, accessed 19 Jun 2018.

68 *Products: Technologies Developed*, Centre for AI & Robotics, DRDO Website, https://www.drdo.gov.in/drdo/labs1/CAIR/English/indexnew.jsp?pg=products.jsp, accessed on 19 Jun 2018.

69 Richa Bhatia, *If The Future Of Warfare Is With Automated Weapons – Where Does India Stand In The Race*? Analytics India Magazine, 27 Mar 2018, https://analyticsindiamag.com/if-the-future-of-warfare-is-with-automated-weapons-where-does-india-stand-in-the-race/, accessed 19 Jun 18.

70 *India Working on Unmanned Tanks, Vessels, Robotic Weaponry for Future Wars*, The Times of India, 20 May 2018, https://timesofindia.indiatimes.com/india/india-working-on-unmanned-tanks-vessels-robotic-weaponry-for-future-wars/articleshow/64243702.cms.

71 *Draft Defence Production Policy 2018*, Ministry of Defence (Defence Production), Government of India, Mar 2018, pp. 3-4.

72 *Transforming Science and Technology in India*, Economic Survey Report 2018 Vol I Chapter 8, Ministry of Finance, Government of India, pp. 119-130.

73 *Defence Procurement Policy 2016*, Ministry of Defence, Government of India, 2016, pp.191-240.

74 *About DARPA*, Defence Advanced Research Projects Agency, US Department of Defence, https://www.darpa.mil/about-us/about-darpa.

75 *U.S. Electronics Innovation Leaps Forward Via Joint University Microelectronics Program, News and Events*, Defence Advanced Research Projects Agency, US Department of Defence, 17 Jan 2018, https://www.darpa.mil/news-events/2018-01-17, accessed 17 Jun 2018.

76 Farnam Jahanian, *4 Ways Universities are Driving Innovation*, Annual Meeting, World Economic Forum, 17 Jan 2018, https://www.weforum.org/agenda/2018/01/4-ways-universities-are-driving-innovation, accessed 06 Jun 2018.

77 Ibid. 73, pp. 3-4.

78 *Technology Perspective and Capability Roadmap (TPCR) - 2018*, Ministry of Defence, Government of India, https://mod.gov.in/dod/news/technology-perspective-and-capability-roadmap-tpcr-2018-0, accessed 19 Jun 2018.

79 Ibid. 73, pp. 192.

80 *Fact Sheet: Communications-Electronics RDE Centre*, US Army RDECOM Website, https://www.army.mil/e2/c/downloads/419768.pdf, accessed 15 Jun 2018.

81 *Fact Sheet: Army Research Laboratory*, US Army RDECOM Website, https://www.army.mil/e2/c/downloads/-419767.pdf, accessed 15 Jun 2018.