Legal and Policy Implications of Autonomous Weapons Systems

31st October, 2020

Authors: Anoushka Soni, Elizabeth Dominic
Edited and curated by: Arindrajit Basu
Reviewed and edited by: Aman Nair
Research inputs: Anusha Madhusudhan

The Centre for Internet and Society, India
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to the Report</td>
<td>4</td>
</tr>
<tr>
<td>CHAPTER 1: BACKGROUND AND DEFINITIONS</td>
<td>6</td>
</tr>
<tr>
<td>Key Terms</td>
<td>6</td>
</tr>
<tr>
<td>Country Positions</td>
<td>9</td>
</tr>
<tr>
<td>India and Autonomous Weapon Systems</td>
<td>16</td>
</tr>
</tbody>
</table>

| CHAPTER 2: INTERNATIONAL HUMANITARIAN LAW AND AUTONOMOUS WEAPON SYSTEMS | 19   |
| Introduction                                                          | 20   |
| Martens Clause                                                       | 20   |
| International Humanitarian Law                                       | 25   |
| Distinction                                                          | 26   |
| Distinguishing between military and civilian objects                  | 28   |
| Distinguishing between civilians and combatants                       | 31   |
| Distinguishing between civilians and civilians participating in hostilities | 33   |
| Distinguishing between combatants and hors de combat                  | 34   |
| Proportionality                                                       | 35   |
| India and International Humanitarian Law                            | 36   |
| Conclusion                                                           | 37   |
| Meaningful Human Control                                             | 37   |
| Explainable AI                                                       | 40   |

| CHAPTER 3: AUTONOMOUS WEAPONS SYSTEMS AND INTERNATIONAL CRIMINAL LAW  | 44   |
| Introduction                                                          | 42   |
| The Question of Accountability                                       | 42   |
| Liability Regime                                                     | 44   |
| Direct Liability                                                     | 44   |
Indirect Liability 45
Doctrine of command responsibility 45
Why not a criminal negligence standard? 47
Developer Accountability: A Possibility? 48
The Way Forward 1.0: Dynamic Diligence 50
The Way Forward 2.0: War Torts And Dynamic Due Diligence 52
What Is The Way Forward For India? 54
Conclusion 56

CHAPTER 4: AUTONOMOUS WEAPONS SYSTEMS AND THE PRIVATE SECTOR 57

Introduction 57
What’s the Big Deal? 57
A Look Around the World 58
Where Does India Stand? 60
The Divided Stance 62
What Can the Private Sector Do? 64
INTRODUCTION TO THE REPORT

Wars have been a part of human existence from the very beginning. However, the evolution of civilization has led to the evolution of wars. As a society, our discourse is now centred around on how this new generation of wars is best fought rather than whether at all to fight them. This inevitability of war has further led countries to develop means and methods of warfare, for inevitability of war is only acceptable when it is accompanied by the inevitability of victory. Autonomous Weapon Systems (AWS) or Lethal Autonomous Weapons Systems (LAWS) have, in recent times, sparked a global debate regarding what is being called the future of technology: artificial intelligence. In the backdrop of revolutionizing wars, AWS are being developed by certain countries to gain an edge over the others, forcing others to participate in the arms race of the 21st century in order to prevent asymmetric development of warfare. The international community must now contemplate the legal, moral and ethical implications of further developing existing automated weapons and giving them more autonomy than ever before.

It is to ally such concerns that a Group of Governmental Experts (GGE) was convened by the United Nations Convention on Certain Conventional Weapons (UN CCW) in December 2016, clearly demonstrating the global interest in the issue at hand. The Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects or the UN CCW was established with the aim of restricting weapons considered to cause unnecessary suffering and impact civilians disproportionately and indiscriminately.1

This paper is divided into 4 Chapters. Chapter I authored by Anoushka Soni defines and differentiates between certain key terms imperative for a better understanding of autonomous weapon systems in all its technicalities. Further, the Chapter also provides a broad overview of the difference in existing state practice by reviewing the lack of universality of a definition for autonomous weapons. Chapter II also authored by Anoushka Soni analyses autonomous weapons from the perspective of international humanitarian law. It first contemplates the prima facie illegality of autonomous weapons, and subsequently focuses on their lawful use with regard to the principles of distinction, proportionality and military necessity and the conclusion provides a normative look at the way forward. Chapter III authored by Elizabeth Dominic goes into the question of accountability and redress and evaluates models of criminal and civil liability in case autonomous weapons systems go wrong. Finally, Chapter IV authored by Elizabeth Dominic evaluates the role of the private sector in the development, trade and policy framework on autonomous weapons systems around the world.

CHAPTER 1: BACKGROUND AND DEFINITIONS

Key Terms

To understand the international law implications of autonomous weapons, it is first imperative to understand the component of such systems that spark the debate – the ‘autonomous’, or ‘artificial intelligence’ component.

‘Artificial intelligence’ as a subject of research is not new, in fact research into the area began in the mid twentieth century. However, capabilities were limited at that time. The turn of the century brought with it an exponential growth in the foray into AI. This sudden sea change was brought about due to a combination of technological improvements, the prevalence of ‘big data’ and other geo-political reasons that pushed AI to the forefront of the technological sector.² Artificial intelligence, such as the one referred to here, also has no definition. However, Section 238 of the FY2019 National Defence Authorization Act (NDAA) of the United States provides a definition that acts as a broad overview of what AI could possibly include, and defines the same as:

1. “Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
2. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
3. An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
4. A set of techniques, including machine learning that is designed to approximate a cognitive task.
5. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision-making, and acting.”³

---


Simply put, in line with definitions adopted in previous CIS research, a system driven by AI involves the delegation of some form decision-making power to the autonomous system.⁴

Although **Autonomous Weapon Systems (AWS)** lack any globally accepted definition as yet, they are broadly defined as any systems that possess a degree of ‘intelligence’, which is defined to be an objective threshold. By virtue of possessing such intelligence, Autonomous Weapon Systems are able to select and engage targets without requiring human direction or interference. These weapons are categorized as lethal when the targets in question are human beings.⁵ A commonly accepted starting point for the definition of Autonomous Weapon Systems comes from the definition under the United States’ Department of Defense Directive 3000.09, which states:

“[a] weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation.”⁶

However, even today, a plethora of automated machines exist for the sole purpose of replacing human involvement in that particular area. What then makes AWS such a threat that countries are campaigning to ban the mere development of the technology, over regulating its eventual use?⁷ The differentiating factor in case of these Autonomous Weapon Systems comes from the definition of the word *autonomous* as compared to the word *automated*. An automated system functions on a pre-programmed set of if-X-then-Y rules.⁸ This predefined structure with certain definite parameters is required to ensure the predictability of outcomes, barring an unpredicted technological failure. Further, because the rules that have been given to the system are clear, human intervention, if necessary, is an uncomplicated process. Autonomous systems on the other hand, as mentioned above, are equipped with artificial intelligence. The system in this case is expected to learn and correct itself, hence the shift in the field of engineering towards machine learning concepts. Machine learning focuses on the identification of statistical relationships in data. If this data is generated from real world examples, machine learning

---


can be used to create high performing algorithms such as the ones used in Autonomous Weapon systems.

Further, the number of parameters on the basis of which such autonomous systems arrive at their final output far outnumbers those in case of automated systems. Unlike the latter, which produce the same result given identical inputs, autonomous systems may produce a different output even when the inputs provided are identical. Therefore, the predictability that we associate with automated systems potentially reduces as we grant increasing autonomy to the same.

It is clear that recent advancements in cyber security are dependent on the increasing use of machines in war. The varying levels of control that humans exercise over such machines determines the relationship between the two. The level of autonomy granted to pre-existing automated systems is inversely proportional to the level of dependence that these machines have on human direction. If more autonomy is given, it implies that machines make more decisions on their own and are less dependent on humans and vice versa. In fact, in such a scenario, humans rely more on such machines to take actions for them. It is also undeniable that machines do improve accuracy and analyse large quantities of data, thereby reducing human effort. However, the question that has prompted global debate is that the development of technology comes with the consequence that, to replace human soldiers with robotic ones, the lives of people must be put in the hands of machines. This is the reason that questions of ethics, morals, and legality, are increasingly cropping up in international law regarding such systems.

Questions have also been raised as to how autonomy in the critical functions of such systems should be viewed. These systems are developed with the aim that they will be precise and accurate in targeting and human error in judgement would be eliminated. However, scholars argue that human interference is necessary to ensure compliance with the basic principles of international humanitarian law.


While there is increasing debate on AI and autonomous weapon systems, conceptual clarity on various terms surrounding the debate is equally important. The terms ‘computer intelligence’ and ‘autonomous’ are fallaciously used interchangeably. However, an autonomous system does not necessitate intelligence and the mere presence of such intelligence does not imply autonomy of the system. Further, autonomy and autonomous weapons are also terms that have different connotations, which are used interchangeably. The autonomy of a weapons system comes from the level of human engagement with that system. However, artificial intelligence as a concept has no correlation with human engagement and is instead dependent on the capability of the machine to make independent decisions based on a variety of data and input parameters. A lack of a clear universal definition of artificial intelligence and autonomous weapon systems further complicates understanding.

**Country Positions**

Currently the regulation of Autonomous Weapon Systems is proposed to be done under the United Nations Convention on Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (‘CCW’).¹⁴ The first time such weapon systems were brought within the ambit of the CCW was 2014, when the first Meeting of Experts on Lethal Autonomous Weapon Systems was set up.¹⁵ In 2016, the High Contracting Parties to the CCW decided to set up a Governmental Group of Experts to discuss the emergent area of law in autonomous weapons,¹⁶ and the GGE had its first meeting in 2017.¹⁷ A general exchange of ideas at the first GGE led to differences being expressed in various countries' willingness to pre-emptively ban such weapon systems. The ambiguity around the definition of autonomous weapon systems is evinced by the varying definitions propounded by countries for such systems at such international fora, as well as their domestic law. France and Germany proposed a potential first step in the form of a political declaration that reaffirmed the global community's desire to maintain human control where human lives are concerned as this perhaps the only area of broad consensus.¹⁸ Even here, the degrees of human control stemming from each state’s


¹⁶ CCW/CONF.V/2 - 2016, Report and recommendations of the Informal Meeting of Experts


¹⁸ Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious
threshold and definition of human control differed. Various ideas were proposed, for instance the EU along with a few others proposed national weapon reviews to establish information exchanges and best practices based on the same.19

Another question on which countries differed were what parameters were required to classify a weapon as an autonomous weapon system. An overview of various countries’ definitions of autonomous weapon systems is given below to explain the lack of global consensus that still persists on the matter:

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>DEFINITION OF AUTONOMOUS WEAPON SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>CUBA</td>
<td>“Fully autonomous weapons should be understood as those who act without human supervision once they are deployed. The semi-autonomous weapons must be understood as those with the supervision of a human operator, at least in its critical functions, that is to say for selection and attack of targets.”20</td>
</tr>
<tr>
<td>CHINA</td>
<td>“LAWS should include but not be limited to the following 5 basic characteristics. The first is lethality, which means sufficient pay load (charge) and for means to be lethal. The second is autonomy, which means absence of human intervention and control during the entire process of executing a task. Thirdly, impossibility for termination, meaning that once started there is no way to terminate the device. Fourthly, indiscriminate effect, meaning that the device will execute the task of killing and maiming regardless of conditions, scenarios and targets. Fifthly evolution, meaning that through interaction with the environment the device can learn autonomously, expand its functions and capabilities in a way exceeding human expectations.”21</td>
</tr>
<tr>
<td>ESTONIA &amp; FINLAND</td>
<td>“Due to the many effects and implications of advanced machine autonomy in association with weapon systems, even a working definition of LAWS is very difficult to frame. To complicate matters further, each word in the scoping phrase “lethal</td>
</tr>
</tbody>
</table>


“LAWs are defined as fully autonomous lethal weapon systems. Systems such as remotely piloted and automated systems (e.g. conventional charges exploding with a set timer), tele-operated (e.g. drones), automated missile defense systems, torpedoes, guidance and navigation systems, surveillance and detection systems are not considered as LAWs.”

“Fully autonomous weapons would be able to select and engage targets without meaningful human control. They represent an unacceptable step beyond existing armed drones because a human would not make the final decision about the use of force in individual attacks.”

---


<table>
<thead>
<tr>
<th>International Committee of the Red Cross</th>
<th>“Any weapon system with autonomy in its critical functions—that is, a weapon system that can select (search for, detect, identify, track or select) and attack (use force against, neutralize, damage or destroy) targets without human intervention.”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netherlands</td>
<td>“A weapon that, without human intervention, selects and engages targets matching certain predefined criteria, following a human decision to deploy the weapon on the understanding that an attack, once launched, cannot be stopped by human intervention.”</td>
</tr>
<tr>
<td>Russia</td>
<td>“Autonomous weapons system— an unmanned piece of technical equipment that is not a munition and is designed to perform military and support tasks under remote control by an operator, autonomously or using the combination of these methods.”</td>
</tr>
<tr>
<td>Switzerland</td>
<td>“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.”</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>“An autonomous system is capable of understanding higher-level intent and direction. From this understanding and its perception of its environment, such a system is able to take appropriate action to bring about a desired state. It is capable of deciding a course of action, from a number of alternatives, without depending on human oversight and control, although these may still be present. Although the overall activity of an autonomous unmanned aircraft will be predictable, individual actions may not be.”</td>
</tr>
<tr>
<td>United States of America</td>
<td>A weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation.</td>
</tr>
</tbody>
</table>

The 2017 GGE concluding report reaffirmed that international humanitarian law applied to all weapon systems and thus includes autonomous weapon systems within its ambit.  


27 Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious...
Further, consensus was reached as to the fact that research and development of these technologies for civilian benefit purposes should not be hampered by steps taken to regulate autonomous weapon systems. Along with this, areas that the group disagreed upon such as certain aspects of development, deployment and the requisite human-machine interaction, including but not limited to the extent of human control, of these systems were left open to future discussion.

Each country’s definition of an Autonomous Weapon System reflects, to a certain extent, their position on the matter. China for instance put forth the aforementioned definition in its April 2018 GGE position paper, around the same time they announced their “desire to negotiate and conclude”. On the same day, the Chinese Air Force announced its intention to cooperate with various private universities on a competition, the purpose of which was - “focus on the assessment of the intensive formation of UAV clusters, high-speed precision obstacle avoidance, collaborative search identification and positioning, cluster coordination strategy and dynamic mission planning.”. The inherent contradiction in these two announcements led most nations to believe that though China may advocate for limiting the use of LAWS, they will continue to develop their own capability.

A small but powerful bloc of the United States, United Kingdom, Israel, France and Russia along with a few others have argued against a premature ban on Autonomous Weapon Systems. Each of them hold their positions for a variety of reasons.

On a domestic level, the Department of Defence of the United States has introduced Directive 3000.09 which makes the country one of the few to implement domestic regulations on the issue of semi-autonomous and autonomous weapon systems. US international negotiations are aimed at moving towards an implementation of their domestic policy at an international level. They have submitted three Working Papers at the Group of Governmental Experts (GGE) meetings that detail their position on the matter. The definition mentioned above was introduced in the Directive. The Directive mandates a level of human involvement when lethal force is required to be applied, thus allowing for the human operator to make the final call regarding the decision making.

To understand the US position on autonomous weapon systems, it is imperative to understand the reason that such systems have sparked such fierce debate. The primary reason is due to the lack of human decision making, which is evident from each country’s definition of what an Autonomous Weapon System is. Any weapon system has four tasks that it performs – searching for a particular target, detecting the target, deciding whether


29 Supra, n. 26.

to engage the target and eventually engaging the target. Colonel John Boyd defined these 4 actions taken in competitive decision making: observe, orient, decide and act – the OODA loop. If a human operator is operating the weapon system, all these steps are taken by the operator. However, as machines are given a greater degree of autonomy, the human operator relinquishes some, eventually possibly all, functions in the loop to the machine. The crux of the debate lies in answering the question - how much of control should be relinquished?

THE OODA LOOP

Therefore, if we were to refer to this OODA loop, the US position would imply that the human operator relinquishes control to the machine for observing and orienting, however the final decision and subsequent action or lack thereof is given to the human operator.

At a policy level, the United States believes that it is unnecessary for the GGE to adhere to a particular definition of LAWS, and instead prefers a general understanding of their characteristics. If a specific legal definition was to be adopted, it would be done so for the purposes of a legal rule. Legal definitions are often determinant of the scope of the legal rule in question. Due to the current divide in the GGE, it is believed that if a working definition was adopted it would be done so to cater to the particular legal rule of banning the development of autonomous weapon systems. Therefore, the USA is opposed to the adoption of one in the belief that it would take away from what the issues are which are covered by this debate. This is in tandem with their belief that the benefits of the technology, such as greater military precision and the consequential reduction in civilian

---


casualties, outweighs the finality of such a ban especially when the technology is currently in its nascent stages.  

France has largely advocated against a pre-emptive ban on autonomous weapon systems. However it has been forced to play mediator in the past few years to aim to bridge the gap on an issue that has prompted deep divides over the same. They have also drawn fire over their seemingly contradictory positions as the French Ministry of Armed Forces maintains that ‘killer robots’ should not be allowed to emerge while simultaneously developing programs with increasing levels of autonomy.

Germany has been struggling with an internal divide regarding autonomous weapon systems. Since World War II Germany has prided itself on establishing itself as a 'civilian power' with diplomacy as its strongest weapon. However, the recent debate around the development of artificial intelligence is not one that can be limited by its dual military and civilian use capabilities. AI will play an important role in all sectors of an economy and as a result a ban on LAWS may mean that progress in civilian use of the same technology will be hampered. The European Union also emphasized this point at the 2017 meeting of the GGE, and on various occasions since. In maintaining a balance between not wishing to favour military developments and yet retain the capability to do ground-breaking AI research, Germany took the path of least resistance in supporting France and asking for a political declaration. This was done in hopes of forming a French-German position on the issue, as is evident from their joint definition provided


above. The Campaign to Stop Killer Robots and other proponents of a ban believe that this measure may be adopted by multiple nations with the intention of making this the final point of discussion on the issue and that is seen as less than a ban, regulation or even a treaty.\(^{39}\) As a result, they criticized Germany for toeing the French line, and not developing their own position, preferably in a European Union context.\(^{40}\)

The United Kingdom’s aforementioned definition of Autonomous Weapon Systems is a futuristic definition of what these systems may be capable of if developed to their full capacity. The UK government has expressed its doubts that such fully autonomous weapons will exist in the near future. The UK’s definition of AWS demands a degree of sophistication in these systems that they do not currently possess and as such their position on weapons with a lower degree of sophistication is hard to discern.\(^{41}\) Further, the Defence Ministry has guaranteed human oversight, authority and accountability in the operation of all UK weapon systems. However, critics of such systems have observed that by setting the threshold for what constitutes LAWS so high, the UK is effectively giving a green light to development of systems that do not meet this threshold.\(^{42}\)

**INDIA AND AUTONOMOUS WEAPON SYSTEMS**

India is an emerging player in the global arena and its technological capabilities are still limited. As an arms importer, it must consider the trade implications along with national security implications of global advances in the development of autonomous weapon systems. As a result, it’s position on autonomous weapon systems stems from what it may mean for the growth of asymmetric warfare globally if countries that possess the technology to develop such systems continue to do so.\(^ {43}\) Further, the compliance compatibility of international humanitarian law and autonomous weapon systems was also questioned.

The idea that autonomous weapon systems would reduce the threshold for countries going to war due to the lack of civilian casualties involved has been put forth by many

---


\(^{40}\) Id.


advocates of a ban on autonomous weapon systems. In 2016, India’s Permanent Mission to the Conference on Disarmament made a statement at the CCW Informal Meeting of Experts on Lethal Autonomous Weapon Systems whereby India expressed concerns over the same. In addition to this, they have pointed out the divide that exists in the country's positions on key issues. This includes questions such as when a weapon becomes a new weapon and thereby a new method of warfare for the purpose of regulation, national reviews etc.

The aforementioned 2016 statement ends with the telling phrase “in these circumstances, it may be prudent not to jump to definitive conclusions”. Evident from this, India's wait-and-watch approach could be interpreted as their lack of support for the pre-emptive ban on such weapon systems which implies a degree of finality. This theory is supported by the fact that India has also stressed upon the dual military and civilian use of this technology. Further, the Defence and Research Organization (DRDO) had in 2013 publicized the fact that they were developing robotic soldiers with a self-purported high level of intelligence and distinction capabilities, and that work was underway on the same for deployment by 2023. In 2018, the Prime Minister had also laid emphasis on the importance of AI and robotics for global defence forces.

India's geo-political scenario, being surrounded by two hostile nations, is another reason why if autonomous weapon systems are indeed the arms race of the 21st century, India can't afford to fall behind. China’s contradictory and uncertain position on Autonomous Weapon Systems has been highlighted above. Pakistan on the other hand, has strongly advocated in favour of the pre-emptive ban on such systems. However, the Indian government is wary at taking Pakistan at face value, considering the fact that they had previously called for a nuclear free South Asia and yet continued to develop its own nuclear weapons. This is compounded by the issue of Pakistan using drones to drop weapons into India's border, even though the army claims that they possess the radars to detect and destroy the same.\textsuperscript{44} Therefore, India must consider the benefits of deploying autonomous weapons to safeguard its borders against infiltration attempts and protect its soldiers from the extreme weather conditions. It is to this end that India recently announced the use of mechanised formations such as tanks and infantry combat vehicles.\textsuperscript{45} These will be deployed along certain volatile areas of the border shared with Pakistan and China and minimize the need for risk human lives due to the volatility and weather conditions in such areas.

Autonomous surveillance and combat systems along with adaptive communication systems would prove to be a huge asset in this area. Another aspect of consideration in favour of India’s lack of support for a ban that has been suggested is that such weapon systems may be imperative in protecting the country’s rapidly growing space assets


during potential space conflicts. In India's specific context, the Chinese ability to destroy satellites is well known and thus to ensure protection on all frontiers, they could use autonomous systems as an effective countermeasure.

However, it is also important to consider the asymmetry of warfare if other countries were given free rein in developing such weapons capabilities. It would imply that the current technological lag and thus inherent delay in the development of autonomous weapon systems that exist shall persist because there would be no threshold or cap to signify a finish line. Therefore, although India may not be in favour of a pre-emptive ban on autonomous weapon systems, it should argue for regulation of the same so as to provide itself with an even playing field in its development.

India's position may also be reflected in the Non Aligned Movement's (NAM) position on the issue and vice versa. The NAM has also not been an advocate of a total pre-emptive ban on autonomous weapon systems and has instead directed its focus towards its objective of implementing a legally binding instrument. However, they have called for moratorium on the development of Autonomous Weapon Systems until a legally binding instrument has been set into place. Further, they support the fact that states have arrived at a broad consensus on meaningful human control and wish for this to be a core part of the legal instrument.

Varying country positions on the legality of autonomous weapons are only compounded when the principles upon which such legality depends are analysed. These come from the Law Of Armed Conflict or International Humanitarian Law.
CHAPTER 2: INTERNATIONAL HUMANITARIAN LAW AND AUTONOMOUS WEAPON SYSTEMS

Anoushka Soni

INTRODUCTION

While the understanding of autonomous weapon systems and the global debate surrounding it is essential, the next step is understanding whether the development and use of such weapon systems is permissible under international law. New developments in technology, especially weapons, have throughout history led to a review of existing legal frameworks.\(^{46}\) This is done with the objective of determining whether the current framework is equipped to regulate these new developments or whether a new one is required for comprehensive regulation of the same.

To regulate the use of technological developments in warfare, two kinds of rules are formed. First, in instances where the weapon developed is seen to be \textit{prima facie} unable to comply with IHL, absolute prohibitions have been developed. Consensus has developed over what kind of weapons are legal under IHL and the same is used to determine whether a weapon itself is lawful. The ban on the use of poison on the battlefield, for instance, is a result of these regulations.\(^{47}\) For autonomous weapons, unlike past use, such prohibition is not evident from the nature of technology itself, and therefore those advocating for such weapon systems to be declared illegal use the Martens Clause to do so, which is best suited to combine the ethical debate surrounding autonomous weapons with the legal regulatory framework. The second is conventions on use of weapons, which determine whether the use of a weapon in a particular situation in combat is legal. An analysis of autonomous weapon systems focusing on their technological capabilities would determine their compliance with international humanitarian law as it exists today. A frame of reference can be drawn from the International Court of Justice (ICJ) which has made clear that international humanitarian law applies to all forms of armed conflict and thus all weapons, “those of the past, those of the present and those of the future” are covered under the same.\(^{48}\)

This Chapter is divided into two parts. \textbf{Part I} analyses the arguments for \textit{prima facie} illegality of autonomous weapon systems due to their inherent inability to comply with


\(^{48}\) Legality of the Threat or Use of Nuclear Weapons Advisory Opinion, 1996 ICJ. p. 226.
the provisions of the Martens Clause. Subsequently, Part II analyses the principles of distinction and proportionality in international humanitarian law to provide a framework for their lawful use.

**Martens Clause**

Severe critics of autonomous weapon systems argue that these systems are inherently illegal, the threshold for which is extremely high in international law. They also invoke the Martens clause on the grounds that if there exists no framework under international humanitarian law able to regulate autonomous weapon systems, such regulation should be done as per the dictates of principles of humanity and public conscience. The Martens clause, which introduced these phrases into international law, is responsible for the introduction of ethics into international humanitarian law.  

The Martens clause was first introduced by Fyodor Fyodorovich Martens for the purpose of being used in the preamble of the Hague Convention II of 1899. Since then, the clause has been codified in the Additional Protocol II to the Geneva Convention, Article 1 of which reads:

“In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from dictates of public conscience.”  

The moral, legal and ethical implications of autonomous weapon systems are still being debated at a global level. The Martens clause has always been a universal point of reference in the context of new developments, technological or otherwise. The advocates of a pre-emptive ban on such weapon systems believe that if technological developments are to progress as is, then one day they society shall reach a point where machines are making life and death decisions. As a result, they raise the ethical questions of whether at all a machine system should be tasked with the use of such lethal force. Were this to happen, even if in compliance with IHL, it is argued that the battlefield concept of appealing to the humanity of the enemy is automatically denied to the people facing death at the hands of a machine. Therefore, if a machine is allowed to use lethal force, it

---


51 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, June 8, 1977, 1125 UNTS 609.

must be in compliance with the rules of international law, which implies it must comply with the Martens clause.

This is made harder by the fact that the universality of the Martens clause comes from its broad and non-threatening nature. If countries were to use the Martens clause to pre-emptively ban autonomous weapon systems, it would lead to divisive global debates regarding the legal substance of the Martens clause. The clause, being necessarily broad in nature, can be interpreted narrowly or widely since there is no one accepted interpretation. Even the International Court of Justice in its 1996 Nuclear Weapons Opinion, although dealing with numerous possible interpretations of the Martens clause, did not provide a clear interpretation of the clause. The court merely stated:

“Finally, the Court points to the Martens Clause, whose continuing existence and applicability is not to be doubted, as an affirmation that the principles and rules of humanitarian law apply to nuclear weapons.”

State submissions in the same case however, revealed some State interpretations of the clause that may become relevant in the context of autonomous weapon systems as well. For instance, Russia is part of the bloc of nations arguing against the pre-emptive ban on autonomous weapon systems. Their submissions during the formulation of the 1996 Opinion had argued that the Martens clause was irrelevant because there already existed a separate comprehensive law of war and as such, the clause itself added no more than normative value. The United Kingdom also forms part of the same bloc and had at the time argued that merely due to lack of legal prohibitions, nuclear weapons cannot be said to be lawful. However, they added to that by saying that this lack of legality does not automatically stem from the Martens Clause. Instead, the weapons must not be able to conform to international rules of armed conflict in order to be characterized as illegal. Therefore, they reduce the Martens Clause to a narrow version of its interpretation by arguing that it is a mere reminder of positive duties of states.

Those arguing in favour of a ban on autonomous weapon systems expand it to its widest possible ambit, which implies that the clause brings its own additional requirements to the law of armed conflict. Therefore, under this interpretation, the requirements for an autonomous weapon system to be deployed in battlefield legally are twofold:

1. An autonomous weapon system would have to fulfil the requirements on international humanitarian law and laws of armed conflict as they stand, and
2. Additionally, they would also have to comply with the principles of humanity and public conscience under the Martens Clause.

The first narrower interpretation envisions the second condition of the clause as automatically satisfied upon the satisfaction of the first, whereas the broader one demands that the Martens Clause provide its own normative guidelines and makes the second condition also a substantive requirement. However, an important observation is

53 Legality of the Threat or Use of Nuclear Weapons Advisory Opinion, 1996 ICJ. p. 87.

made in this regard. The threshold for classifying a weapon system as inherently dangerous under is high and few weapons are able to meet this threshold. Therefore, to meet this threshold, proponents of a ban argue that fully autonomous weapon systems, that is, those which lack any form of meaningful human control fail the test of the Martens Clause. They interpret ‘principles of humanity’ to include humane treatment and respect of life and argue that fully autonomous weapons fail this test. This is because such systems lack the compassion required to minimize suffering, which is a requirement for legality of a weapon. Further, if lethal force is entirely in the hands of machines, the ethical question of whether a machine can take a human life arises. Fully autonomous systems also imply that the governing principles of distinction, proportionality and necessity which are a prerequisite to would have to be complied with solely by a machine.

In customary international law, a customary norm requires state practice and opinio juris, and can even include activities of inter-governmental and non-governmental organizations. The International Court of Justice has further clarified that “not only must the acts concerned amount to a settled practice, but they must also be such, or be carried out in such a way, as to be evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it.” Since autonomous weapon systems are still in the development phases, it is argued that customary rules preventing their use have not yet been formed and it thus cannot be prohibited under customary international law.

However, in instances involving custom in international humanitarian law, the obligations that the states follow are primarily prohibitive obligations, therefore, fulfilment of the same requires an omission on behalf of states. Further, since state practice cannot be evidenced from acts on the battlefield due to lack of observability, reliance is placed upon verbal practice. Verbal state practice regarding autonomous weapons is limited to the staunch proponents of a ban, and Jordan, in the August 2019 session of the GGE on

---


58 North Sea Continental Shelf Cases (Federal Republic of Germany/ Denmark; Federal Republic of Germany/ Netherlands) 1969, ICJ.

LAWS added their name to the 29 states that are doing so. It is therefore being argued that *opinio juris* should form the sole basis of customary law regarding autonomous weapons. An analogy can be drawn to the case of prohibition of torture where the ICTY held that though the rule against torture is breached frequently, the number of states advocating for a ban are many and there is no opposition, only violations. A distinguishing factor here however, is the presence of advocates for the development and deployment of autonomous weapons, as evidenced in Chapter I. Therefore, the likelihood of a ban on autonomous weapons emerging from customary law is unlikely.

Additionally, though comprehensive state practice does not exist for review in this regard, certain countries have begun to shift the focus of their military capabilities to the weaponizing of artificial intelligence. Due to the reduced implications on civilian lives, the development of autonomous weapons for use underwater or in the air has proceeded uninterrupted for decades. The United Kingdom, for instance, has developed an Unmanned Surface Vehicle (USV) with the ability to operate autonomously, along a pre-set and predetermined course. The advanced autonomous technology used to program these, along with safeguards in the form of the ability of such USVs to be remote controlled, ensures their compliance with relevant regulations such as the International Maritime Organization’s COLREGS.

If they are not expressly prohibited by customary international law, then the next step of prohibition is, as argued above, the Martens Clause. However, a legal analysis of the Martens Clause finds that autonomous weapon systems could be used legally. The Martens Clause focuses on the principles of humanity and dictates of public conscience, and gives a chance to those wishing to ban these systems to build a moral and ethical argument around it. But because the Martens Clause has legal connotations, it is not enough to justify the moral tenets of it. The Human Rights Watch in their report ‘Killer Robots Fail Key Moral, Legal Test: Principles and Public Conscience Call for Pre-emptive Ban’ puts forth the aforementioned point regarding lack of compassion leading to

---


61 ANTONIO CASSESE, INTERNATIONAL LAW (2005).


inhumane treatment of others. While this may fulfil a moral definition of 'principles of humanity', a legal definition of the same comes from the Laws of Armed Conflict (LOAC) which requires the use of as much force as is required for legitimate military purpose. The assumption that autonomous weapons would use disproportional or unnecessary force is one that is not based in reality. Human inputs that make weapon systems autonomous would not consist of deploying multiple missiles in place of one. Further, since the technology to make these particular systems fully autonomous doesn’t exist, it is impossible to say that when such technology is developed it would always use excessive force.

The second aspect of the Martens Clause is 'dictates of public conscience'. In the absence of a clear definition of the same, assumptions have been made to equate the same with public opinion. The Human Rights Watch report refers to organizations – international and non-governmental that have called for a pre-emptive ban. They have also referred to the Campaign to Stop Killer Robots which has the support of 28 countries, 86 NGOs, 25,000 Artificial Intelligence experts, the European Parliament, and 21 Nobel Peace Laureates. They also conducted a poll showing 61% of the general public in the 26 countries that support them, support a pre-emptive ban. However, because the notion of what public conscience actually entails is broad and vague, it has been argued to be impractical to use. This is because if public opinion is the touchstone to entirely ban the use of autonomous weapon systems, a threshold for the same must be set. Questions have therefore been raised as to whether we can at all use public conscience to ban autonomous weapons, especially when it is more definitively against nuclear weapons which continue to dominate the arms sphere? Therefore, it is impossible to say that autonomous weapon systems violate this aspect of the Martens Clause due to the divisive


72 Christopher J. Greenwood, Historical Development and Legal Basis in THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW (2nd Ed., Dieter Fleck)
public opinion in this regard, which is compounded by the inherently vague nature of the requirements under it.\textsuperscript{73}

Furthermore, the broader interpretation of the Martens Clause is also one that must be adopted with caution. The implication of making the clause a separate requirement independent of IHL implies that the fulfilment of the rules of IHL does not necessarily imply conformity with dictates of public conscience and principles of humanity. Since the proponents of the ban centre their arguments on the premise of fully autonomous weapon systems, the question that arises is, under the broader interpretation of the Marten’s Clause, whether if a fully autonomous weapon systems is developed that does in fact conform to the requirements of IHL, would it still be prohibited? While this would certainly raise arguments in the sphere of international criminal law, due to a lack of clarity as to accountability, the prohibition of the same must not come from the Martens Clause. IHL is premised entirely on the protection of civilians, targeting solely of military objects, and prohibition of use of indiscriminate and uncontrollable force. Therefore, IHL itself complies with the requirements of the Martens Clause and the clause must be viewed as being of perambulatory character to the rules of IHL.

\textbf{INTERNATIONAL HUMANITARIAN LAW}

The debate surrounding the applicability of international humanitarian law is outside the scope of this paper. However, the 2018 GGE Report was unequivocal in stating that “International humanitarian law continues to apply fully to all weapons systems, including the potential development and use of lethal autonomous weapons systems.”\textsuperscript{74} Targeting law provides three primary governing principles of armed conflict – distinction, proportionality and necessity.\textsuperscript{75} For an autonomous weapon system to be legal, it must be able to fulfil all these basic requirements by the requisite parameters being programmed into them or by exercising enough meaningful human control that the burden of compliance shifts to the human. The weapon system must be able to be directed in a manner that focuses only on military objectives and combatants, the expected harm from the same must be proportionate to the advantage gained and the impact on civilians must be minimized.\textsuperscript{76} A culmination of these three factors will decide whether

\textsuperscript{73} Id.


autonomous weapon systems, as a whole or some applications of it, are legal.

Distinction

Distinction as a principle of armed conflict arose from the need for soldiers to distinguish between military and civilian objects so as to avoid unnecessary and indiscriminate killing and destruction of objects. The principle of distinction has been extended to distinction between combatants and civilians, active combatants and those injured (hors de combat). Civilians are granted protection till such time that they do not play a direct and active role in the hostilities.

The principle was first established by the St. Petersburg Declaration which stated that the only object that was recognized as legitimate during war time was to weaken the military forces of the other side. It has since been codified in Article 48, Article 51(2) and Article 79 of the Additional Protocol I of the Geneva Convention. Article 48 states:

“In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.”

Article 51 focuses on the effect of the weapon being uncontrollable, such a biological or chemical weapon which cannot be controlled and defines such acts as:

“4. Indiscriminate attacks are prohibited. Indiscriminate attacks are:

a. Those which are not directed at a specific military objective;

b. those which employ a method or means of combat which cannot be directed at a specific military objective; or

c. those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

5. Among others, the following types of attacks are to be considered as indiscriminate:

a) an attack by bombardment by any methods or means which treats as a single military objective a number of clearly separated and distinct military objectives located in a city, town, village or other area containing a similar concentration of civilians or civilian objects; and

---


78 Id.

79 Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Saint Petersburg, December 11, 1868.
b) an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.”

Other treaties have been formed on the basis of this principle, for instance the Hague Regulations do not explicitly talk about distinction but apply its tenants in Article 25 which prohibits attacking undefended buildings.80

The Rome Statute, parent statute of the International Criminal Court solidifies “intentionally directing attacks against the civilian population as such or against individual civilians not taking direct part in hostilities” into a war crime.81 In the Nuclear Weapons case of 1996, the International Court of Justice referred to the principle of distinction as one of the cardinal principles of international humanitarian law, as well as of international customary law.82 Jurisprudence of the International Criminal Tribunal for the Former Yugoslavia83 and of the Inter-American Commission on Human Rights84 further enshrine the principle into international law.

In the context of weapon systems, State practice, and accompanying opinio juris, has established that weapons which are by nature indiscriminate are prohibited and thus this is binding as customary international law.85 Various bodies such as the United Nations General Assembly86 and the Organization of American States (OAS) General Assembly87 have adopted resolutions to this effect. Military manuals of various countries have also prohibited the use of such weapons.88 Therefore, it is well established that autonomous weapon systems must fulfil the principle of distinction or risk being classified as illegal per se.

---

80 Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, October 18, 1907.
82 Legality of the Threat or Use of Nuclear Weapons Advisory Opinion, 1996 ICJ. p. 78.
83 Tadić, 1995, ICTY; Martić, 2003, ICTY; Kupreškić, 2001, ICTY.
The first question is whether at all autonomous weapon systems are ‘weapons’ in the traditional sense at all. To judge the ability of a weapon to comply with the principle of distinction, the nature of the weapon along with its impact are considered. If a weapon by its nature is unable to be used in a manner that complies with this principle, then the weapon is rendered illegal and therefore should be banned. If a weapon can be used in a manner that adheres to the principle of distinction, but its destructive effects are so large that they defeat the purpose of its targeting, then too the weapon violates the principle of distinction and is banned from use in combat. However, in autonomous weapon systems, the level of technology that exists today has not reached the level where the weapon itself has been made autonomous. Rather, these systems, equipped with a large variety of sensor configurations and high speed information processing guide the use of multitudinous weapons in combat. Since the weapon does not change, it is likely that the weapon itself will pass the distinction test, even though the system controlling it may not. Therefore, a comprehensive test of distinction would require a shift from viewing the weapon as an instrument or its destructive impact to a focus on the process by which the use of force through it is initiated.\(^9\)

For determining whether an Autonomous Weapon System is capable of complying with the principle of distinction, the components of distinction become relevant. Distinction can be broken down into being able to distinguish between military and non-military objects, between combatants and civilians – an essential component of which is being able to identify those civilians directly participating in hostilities; and to refrain from attacking the injured or hors de combat.

**Distinguishing between military and civilian objects**

For an autonomous weapon system to be able to distinguish between military and civilian objects, it must adhere to Article 52 of Additional Protocol I of the Geneva Convention which states:

1. “Civilian objects shall not be the object of attack or of reprisals. Civilian objects are all objects which are not military objectives as defined in paragraph 2.
2. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.
3. In case of doubt whether an object which is normally dedicated to civilian purposes, such as a place of worship, a house or other dwelling or a school, is being used to make an effective contribution to military action, it shall be presumed not to be so used.”

Therefore, Article 52 prescribes a 2 part test for what constitutes a military objects:

1. The object in question must effectively contribute to military action and
destruction by virtue of their nature, location, purpose or use, and
2. Total or partial destruction, capture or neutralization of the object must offer a
military advantage.

To ensure that AWS passes the Article 52 test, they would first need to be able to identify
what a military object is. Common and obvious military objects like fighter jets, tanks, etc.
are easily identifiable and hence can be programmed into the system to fulfil the
principle of distinction. However, some objects are not easily identifiable as military
objects, such as usually innocuous objects used for military purposes. To make a
determination as to these objects, the system must be able to able to combine its
analysis of an object’s nature, location, purpose or use and make a determination as to
whether an object is a military object or not:

1. **Nature**: Nature of a military object can be used to define all objects that are put to
direct use by armed forces. These include weapons, sleeping barracks, depot,
buildings used as headquarters, equipment. All of these are objects and thus it is
possible to program them into a system, and various countries are increasingly
using Artificial Intelligence to develop battlefield mapping systems which will help
in such identification.

2. **Location**: The next requirement is that of location. Location in and of itself has no
discernible military function, however is a crucial factor in combat nonetheless.
For instance, bridges or other such areas can provide crucial points of strategic
advantage. These can be programmed into the system because they are fixed
points determinable in advance.

3. **Purpose**: While nature and location are more objective requirements, purpose or
use is context based. ‘Purpose’ refers to the intended use of a particular object
that may otherwise be ‘used’ for an entirely different purpose. Therefore, ‘use’
implies a present function of an object. The purpose of certain objects can differ
from its use, for instance hospitals, schools etc in warzones can be used to
accommodate troops, or for the opposite side can form safe houses, assuming
that they won’t be attacked on this basis. The determination of the purpose or use
of an object by the other side is an uncertain endeavour which requires human
judgement and as such cannot be programmed into a weapons system.

The second aspect of the Article 52 test is that the autonomous system would need to
decide whether the total or partial destruction, capture or neutralization of the object
offers a definite military advantage. The definition of a military advantage would include
forcing a retreat on the other side or weakening it, which could be translated into
percentages and calculated by the system. The precursor is that the advantage must be
definite in nature, and not a mere possibility. It has been argued that in some cases this
may require assessing of elements that are purely contextual and as such the subjectivity
would not allow for machines to take over the role successfully.\(^9\)

---

Humanitarian Aspects*, (May 9, 2014).
destruction of Object A offers more military advantage than Object B would be changing contextually in a dynamic battlefield and therefore the autonomous weapon system would have to constantly reanalyse the information it receives.

The United States has submitted a Working Paper expressing their belief that AI will improve military awareness of civilians and civilian objects. This is an important consideration because a large number of unintended civilian casualties occur due to the fact that militaries are unaware of the presence of civilians and hence cannot factor it into their decision making regarding engaging with a particular target. At a domestic level, the US Department of Defense is experimenting with the aim of using AI to improve video analysis from ISR (Intelligence, Surveillance and Reconnaissance) platforms.

The definition of military objective is expressed in broad terms because further precision comes only from the context in which it is used in. This has thus been used to suggest that autonomous weapon systems cannot comply with this because they require a degree of precision to operate. Along with this, even quantifiable parameters like military advantage require a dynamic and contextual determination which renders the system ineffective.

These critiques are done by proponents of a pre-emptive ban to suggest that it is impossible for such weapon systems to comply with international humanitarian law and they are thus illegal. However, the requirements of clause 2 of Article 52 are accompanied by clause 3 which requires forbearance in cases of uncertainty. Therefore in cases of purpose or use when the machine is unable to make a determination, the weapon system would not be illegal for failing to comply with the principle of distinction, it would just arrive at the conclusion not to fire. At this point, human control could play a significant role and could in fact have the final say in whether or not to fire. If the argument made is that in cases where purpose or use is contextual, human judgement and experience is required, then having human intervention at this stage provides a plausible solution to the same. However, this is subject to the fact that the autonomous system in question can detail the parameters which led to it taking a particular decision. Most systems have a ‘black box’ which prevents the human operator to understand the factors considered by

---


93 Supra, n. 30.

94 Supra, n. 26.


\textbf{Distinguishing between civilians and combatants}

Article 48, as given above, codifies the principle that attacks can only be directed against combatants and civilians are thus protected from the same. Further, medical and religious personnel, even if members of the opposing force are protected.\footnote{Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention), October 21, 1969, 75 UNTS 31. Article 25.} However, the protection to civilians and medical personnel is only extended until they are found to be directly participating in hostilities, at which times they may be lawfully targeted.\footnote{ICRC, \textit{Rule 3: All members of the armed forces of a party to the conflict are combatants, except medical and religious personnel}, available at <https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rule3#Fn_2751A918_00002> . Last accessed 16th October, 2019 ; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 UNTS 3. Article 51, para 3.} The principle of forbearance that applied in case of distinguishing between objects also applies here. The ability of an autonomous weapon system to distinguish between the two depends on the definition of a combatant and civilian.

According to the Additional Protocol I of the Geneva Convention, combatants may be defined as:

“\textit{The armed forces of a party to a conflict},” and also

“\textit{Groups and units that are under a command responsible to that party for the conduct of its subordinates, even if that party is answerable to a government or an authority not recognized by an adverse party. Such armed forces shall be subject to an internal disciplinary system, which, inter alia, shall enforce compliance with the rules of international law applicable in armed conflict.”}\footnote{Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 UNTS 3. Article 43.}

Customs have been developed in international law to identify combatants, which are as follows:\footnote{Id.}

\begin{enumerate}
\item As a collective entity, they must be subordinate to a party to the conflict, and as such be a subject of international law
\item The collective entity must be an organization of military nature
\item There must be a commander exercising efficacious control over the members of the entity
\end{enumerate}
4. They must comply with the rules of armed conflict and international humanitarian law.

Article 50 of the Additional Protocol I defines ‘civilians’ and ‘civilian population’ as follows:

1. “A civilian is any person who does not belong to one of the categories of persons referred to in Article 4 A 1), 2), 3) and 6) of the Third Convention and in Article 43 of this Protocol. In case of doubt whether a person is a civilian, that person shall be considered to be a civilian.
2. The civilian population comprises all persons who are civilians.
3. The presence within the civilian population of individuals who do not come within the definition of civilians does not deprive the population of its civilian character.”

Article 51 further lays down guidelines for the protection of civilians by ensuring that the civilian population and individual civilians are protected against the dangers of military operations. Further it prohibits civilians being the object of attack and acts or threats done with the intention of spreading fear among them are explicitly prohibited.

Subsequently, Article 35 of the Geneva Convention 1977 was adopted, which providing three broad and all encompassing principles regarding the methodology of warfare:

“1. In any armed conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited.
2. It is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering.
3. It is prohibited to employ methods or means of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment.”

Similar to the case of concluding whether a particular object was military or not, here too the autonomous weapon system would have to analyse all the aforementioned factors and make a determination. However, they can only identify those criteria which are visibly identifiable. In the traditional forms of warfare with uniformed combatants, it would be easier for an autonomous system to be able to identify an enemy soldier. As methods of war change, as do the parties involved in conflict, from State to non-state actors, identification becomes increasingly harder. Further, conflicts have started to increasingly shift into cities that are populated with civilians and with a concomitant increase in civilians participating in hostilities, identifiable factors like uniforms have become...
increasingly rare.

**Distinguishing between civilians and civilians participating in hostilities**

Article 51(3) renders civilians unable to take the protection of international humanitarian law and states:

“Civilians shall enjoy the protection afforded by this Section, unless and for such time as they take a direct part in hostilities.”

The problem of identification is only magnified where civilians directly participating in hostilities are concerned. The International Committee of the Red Cross has laid down certain guidelines for what constitutes ‘direct participation in hostilities’:

1. “The act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury or destruction on persons or objects protected against direct attack;
2. There must be a direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part; and
3. The act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another. Measures in preparation of a specific act of direct participation in hostilities, and the deployment to and the return from the location of the act also form an integral part of that act. When civilians cease their direct participation in hostilities, they regain full civilian protection against direct attack.”

These criteria however are all subjective and as a result, programming them into an autonomous system which requires definite parameters to make evaluations is unfeasible. Further, IHL imposes an obligation on States to take all available precautions to ensure prevention of disproportionate damage to civilians, and scholars have questioned whether removal of the human element from weapon systems would ever ensure compliance with the same.

---

105 Id.


**Distinguishing between combatants and hors de combat**

Article 41 of the Additional Protocol I of the Geneva Convention prohibits attacks directed at *hors de combat*, and states, in sub paragraph (2):

“A person is ‘hors de combat’ if:

a. he is in the power of an adverse Party;
b. he clearly expresses an intention to surrender; or
c. he has been rendered unconscious or is otherwise incapacitated by wounds or sickness, and therefore is incapable of defending himself; provided that in any of these cases he abstains from any hostile act and does not attempt to escape.” \(^{108}\)

A common thread across all identifying factors in what defines a *hors de combat* is that the person in question is ‘defenceless’ and thus protected by international law regardless of whether he’s laid down arms or not. \(^{109}\)

Identification also requires interpretation of individual intentions and actions. An example commonly given is detecting a person’s willingness to surrender. The determination of whether indeed a person is willing to surrender requires contextual human judgement. This is complicated by the fact that there exist no guidelines that detail how a surrender should take place. The classical examples of waving a white flag or laying down arms do exist, however, in some cases that is not possible, which is where human intervention is required. It has been argued that the weapon system cannot take these judgement calls and thus it is impossible to use a weapon system in combat that adheres to Article 41. \(^{110}\) Further, doubts have been raised as to whether all surrender is possible to a machine system because of the obligations that exist under international law at the time of such surrender. \(^{111}\)

In identification of *hors de combat* too when there is doubt, forbearance must be observed. Human doubt is one that is recognizable, and is one that causes hesitance before attacking. While algorithms that measure doubt are possible in theory, one that is able to do this alongside factor in the contextual peculiarities of a particular situation is hard to imagine. \(^{112}\) Even if such an algorithm is possible in theory, a threshold for doubt must be set by a human operator. Human doubt can be reasonably categorized as a feeling. To quantify this into a machine would require giving the machine a threshold. If,

---

\(^{108}\) Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1), 1997, Article 41.


\(^{111}\) Id.

say, a 51% chance of success is set as the threshold for having no doubt, this implies a 51% chance of success or a 49% chance of failure. Further, human operators have taken tougher calls with lower odds based on years of experience and intuition which cannot be programmed.

Proportionality

The rule of proportionality is the second requirement for Autonomous Weapon Systems to fulfil the requirements of legality under international humanitarian law. Article 51(5)(b) and Article 57 of the Additional Protocol I of the Geneva Convention together codify the rule of proportionality. Article 51, in defining what types of attacks constitute indiscriminate attacks, includes:

“an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.” ¹¹³

Article 57 lays down certain precautions to be taken during attacks and states:

“refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated;”¹¹⁴

Article 8 of the Rome Statute makes intentionally launching attacks with the knowledge that the damage to civilians or chronic widespread damage to the natural environment outweighs the military advantage gained a war crime.¹¹⁵ When the principle was adopted, it was met with no reservations since most states viewed it a codification of one of the basic tenets of international law. The principle in essence lays down the contours for what constitutes lawful incidental damage and civilian casualties under international law. In submissions of states before the ICJ in the Nuclear Weapons Advisory Opinion and subsequently in the judgement, the principle of proportionality was invoked to assess the compliance of such weapons with IHL. The court acknowledged the same, emphasizing on the respect for environment and its importance in compliance with the proportionality requirement.¹¹⁶

¹¹³ Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1), 1997, Article 51(5)(b).
¹¹⁴ Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1), 1997, Article 57.
¹¹⁸ Legality of the Threat or Use of Nuclear Weapons Advisory Opinion, 1996 ICJ. p. 42.
Proportionality involves an important aspect of calculating the ‘military advantage’ anticipated by an attack. However, there exists a disparity in thought as to whether military advantage refers to gaining military advantage post that particular attack, or military advantage as a whole. Even if autonomous weapons share data, this flow of data needs to account for the dynamic nature of warfare and take into consideration the movement of all the individuals on the field as and when it happens, as the military advantage changes based on this. The ideal way to comply with the proportionality requirement is to therefore ensure that calculations are made on a step by step basis at all levels. For instance, humans can develop a military strategy and ensure that it changes based on the on-ground observations of the AWS. In addition, the use of meaningful human control at the stage of operations of the AI ensures that the human being retains control and ensures accountability in case of technological failure.

The quantification of proportionality however, is not an easy task. The threshold for what constitutes a military advantage has till date been restricted to judgement calls and overall assessment of what a reasonable man would have done in that scenario. However, to program military advantage and define a level will require global consensus at a level that autonomous systems currently do not possess.

**India and International Humanitarian Law**

The legality of Autonomous Weapon Systems is primarily dependent on the weapon’s ability to comply with international humanitarian law (IHL). States that develop such weapon systems must ensure they fulfil the principles of distinction, proportionality and military necessity as laid down in the Geneva Conventions and subsequent Protocols thereto. However, the state’s past record of IHL compliance will be of relevance when determining the principles of IHL the weapon developed by a particular state is likely to comply with. In this backdrop, India has signed and ratified the 1949 Geneva Conventions, however has not done the same with Protocols I, II and III. However, it had passed the Geneva Convention Act, 1960 under Article 253 of the Indian Constitution which prohibited the breach of the Convention and prescribed punishment for the same.

On the specifics of IHL, India, in its written submissions before the International Court of Justice in the Nuclear Weapons Advisory Opinion of 1996 submitted that the use of nuclear weapons under international law is unlawful, as its inability to distinguish between combatants and non-combatants violates customary international law. They have also specifically emphasized the importance of the protection of civilians as a principle of IHL at multiple international fora. Simultaneously however, India has not ratified Protocols I, II and III which pertain to the regulation of non-international armed conflicts under international humanitarian law. With regular political turmoil in the country on religious and communal grounds, the Indian government will likely focus on


120 Id.
developing and deploying autonomous weapons to mitigate the damage caused in such situations as well. However, non-ratification of the Protocols implies that India is unwilling to let those rules govern conflict within its borders. Therefore, it can safely be said that its development and deployment of autonomous weapons on a global scale may conform to the principles of IHL, which is further evident from their active participation in the Governmental Group of Experts of AWS established under the UN CCW.

At a capacity building level, India has formed a task force for ‘Strategic Implementation of Artificial Intelligence for National Security and Defence’. One of the primary aims of this task force is reviewing the ethical, safe, secure and privacy assured use of AI in its military use. However, the conformity of its use of autonomous weapons to police and regulate crime within the country to principles of IHL applicable to non-international armed conflicts is still uncertain.

**CONCLUSION**

This Chapter therefore states and analyses the requirements of international humanitarian law. In most situations requiring distinction and proportionality, the inability of autonomous weapons to comply with these stems primarily from the fact that technology has not evolved to the level where it is capable of making such distinctions. However, the implication of this is not the illegality of AWS, but instead the addition of a crucial component – meaningful human control - to ensure that such systems comply with IHL.

**Meaningful Human Control**

An overarching requirement upon which the legality of autonomous weapon systems under international humanitarian law depends is the concept of meaningful human control (MHC). The requirement of meaningful human control in autonomous weapon systems ensures that the human element, which is essential in the battlefield for factors such as experience, intuition and judgement calls, is maintained. MHC further ensures that autonomous systems combine the efficiency and preciseness of machines with the compassion and experience of human beings.

The questions that arise regarding MHC is at which stage human control is required. The OODA loop, as explained in Chapter I, provides a frame of reference for the same. The first 2 stages of this loop – observe and orient, are inarguably performed better by machines for the main objective behind these stages is data collection, which machines are able to do at a quicker pace than human beings. However, algorithmic biases in such data collection are a real possibility as acknowledged in the 2019 GGE report. The question

---

regarding decisions is both where the functions of autonomy as well as MHC lie. If artificial intelligence is allowed to take such decisions, the technology itself must be capable of complying with IHL, which as established, is not the case yet. Therefore, MHC is required at this stage to ensure IHL compliance. Further, giving machines full autonomy post decision making may prove to be problematic due to the dynamic and ever changing nature of warfare, which may produce unforeseen change in circumstances. The requirement of speed in warfare must therefore must be balanced with the risks associated with warfare, especially when civilians are involved. Machine learning technology, though proving to be efficient in warfare, has also demonstrated unexpected results that would be catastrophic on a battlefield when subjected to adversarial testing.

As a result, MHC is currently seen as the only way to bridge the main divide that exists regarding such weapons at a global stage due to the existence of a base level of consensus on the issue. The MHC necessitates the human control to be ‘meaningful’ which implies that the human control must be of required quality by giving such controllers the requisite training and information. However, the consensus is limited to the fact that meaningful human control must be retained. States continue to differ as to the precise requirements, including what the word ‘meaningful’ implies. The proponents of a ban argue that in cases of autonomous weapons, the removal of humans from the process is incompatible with the IHL obligation to take all feasible precautions to prevent disproportionate damage to the civilian population. On the other end of the spectrum, states argue that ensuring human control at all stages negates the efficiency that autonomous systems were envisaged to bring about in the first place.

In cases of distinction, while it is possible that some kinds of distinction criteria can be fulfilled by the machine, in other cases human control would be a prerequisite for such machines to be legally deployed in combat. However, the nature of human control required has been extensively debated. On one end of the spectrum, Brazil for instance in

---


127 Supra, Schmitt n. 112.
its Working Paper for the 2018 GGE summit expressed its view that autonomy is a function of human control. It also emphasized on the aforementioned point of autonomous weapon systems being legal only so long as they possess an element of human control.\textsuperscript{128}

On the other end of the spectrum, the United States submitted a working paper titled ‘Human-Machine Interaction in the Development, Deployment and Use of Emerging Technologies in the Area of Lethal Autonomous Weapons Systems.’\textsuperscript{129} The paper discusses the US Department of Defence Directive 3000.09 which requires that systems with a level of autonomy – autonomous or semi-autonomous “be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force.” The working paper highlighted the reason for the use of the word ‘appropriate’ which was done in order to emphasize the fact that there is no objective threshold for human control in a particular situation. The level of interaction would differ across the type of weapon system and context of warfare. Further, the level of delegation to machines must also be decided. If human judgement was involved in all aspects, say in all steps of the OODA loop referred to above, it would imply that the increased level of efficiency and precision that stemmed the need to develop such systems would be defeated.

The DoD Directive lays down guidelines for the weapons, their interface with human operators and the human operators themselves. It requires that all such weapons go through various tests, such as hardware and software verification and along with a realistic system developmental and operation test and evaluation. In addition to this, measures will be adopted to ensure that these systems in accordance with their test runs. This will have the necessary consequence of increasing the level of predictability that is lost when a shift towards a greater degree of autonomy takes place. As per the DoD, the tactics, techniques and procedures that will allow these weapons to complete engagements in a timeframe consistent with the intention of the human operator, and upon expiry of such time, terminate the same or seek additional input. Further, robotic failures leading to vulnerabilities in the system or other unintended consequences shall also be minimized. The human operators operating these weapons are trained. In order to facilitate informed decision making in keeping with international law and the rule of engagement, the interface between people and machines for such weapons is required to be easily understandable. It must also provide procedures for the human operators to activate and deactivate the system. This best practice framework is proposed in the US Working Paper at the GGE as well.

The requirement of Meaningful Human Control is facilitated by the recent programs such as the Explainable AI (XAI) program of the United States Defence Advanced Research


Projects Agency (DARPA), which is explained in the following section.

Explainable AI
There are few countries leading the development of AWS currently, and the United States is at the forefront, with Trump recently announcing the “American AI Initiative”. As part of their developments in the field, the Defence Advanced Research Projects Agency (DARPA) of the United States is in the process of developing and testing its Explainable AI program, which aims at enabling artificially intelligent systems to explain their decisions. The level of human intervention in autonomous weapon systems is based entirely on how explainable the AI used by the program is. Explainable AI, though not changing the weapon’s inherent capability to distinguish by design, would allow the operators to understand the program and its limitations better. While testing these systems in a simulated environment, it would now be shown what stimuli the system was able to recognize and prioritize. During this process, by making the simulated environment increasingly dynamic, they could judge as to how the system incorporated the new, fast changing stimuli into its decisions. Further, in the interim while this technology is being developed, the use of autonomous weapon systems can be limited to rural, unpopulated areas or to combat other unmanned systems. As a result, the question about a weapon being illegal for not being able to comply with the principle of distinction is delayed if not removed.

In the cases of situations of distinction between objects that are not easily identifiable, in addition with distinction between civilians, combatants and hors de combat, the likelihood of technology evolving to the level of quantifying these subjective parameters is currently limited. Therefore, in this context, even if Explainable AI becomes a reality, in such cases where it is difficult for even human judgement to make the right call, autonomous weapon systems would be ineffective. Especially in cases of hors de combat, the protection accorded to this category of individuals is high and the objective markers can be easily imitated by enemy combatants, since the machine will itself not be able to distinguish. Therefore, if using Explainable AI, the human controller is better placed to understand the decision of the machine and take the final decision, both compliance with IHL and accountability is ensured.

In case of proportionality, Explainable AI could be a possible solution, but directly quantifying doubt without human intervention is impossible. However, when the AI is able

---


to provide the human operator with the parameters on the basis of which the decisions was taken, it becomes easier for the human operators to incorporate such parameters in their military strategy, thereby enabling both fulfilment of proportionality and accountability as the human operator will take the final call.

It is imperative that autonomous weapon systems not be written off as illegal and immoral, especially considering the nascent stage at which technology is currently at in the field. Though autonomous weapons raise a host of legal and ethical questions, they are also responsible for streamlining the process of decision making in a battlefield. The concept of meaningful human control is likely to guide future debates into autonomous weapon systems as it remains the sole bridge in the divide between. Further, the divide that exists is centred around the development of fully autonomous lethal weapon systems. However, what states are failing to consider at this stage is the use of autonomous weapons need not be restricted to lethal use of force. Autonomous weapons can be used like unmanned submarines in areas where damage to human life is little to none. They can be equipped with non-lethal force and used as deterrents for countries with porous borders. Further, the development of the artificial intelligence component of such a system is technology that possesses both civilian and military use. Were this component developed further, it would bring about advancements such as self-driving cars and other developments for civilian use.

The benefits of AI however, does not mean that the associated risks and costs must be ignored. However, this author believes that with the implementation of meaningful human control to make these systems IHL compliant, the lawful use of such systems is a possibility in modern warfare. IHL is a comprehensive body of law, with rigid rules that ensure fairness and accountability on a battlefield. If autonomous weapon systems can indeed conform to this, then the ethical argument of their inherent illegality stands on unstable legal grounds. Aversion to development of technology has existed from the beginning of time, however, it’s subsequent normalization and incorporation into our day to day lives is also a reality.
CHAPTER 3: AUTONOMOUS WEAPONS SYSTEMS AND INTERNATIONAL CRIMINAL LAW

Elizabeth Dominic

INTRODUCTION

As modern technology is rapidly finding its way to every aspect of our lives, the development of Autonomous Weapon Systems (AWS) increasingly reshaping modern warfare comes with no surprise. From the U.S. Navy’s Phalanx system to Israel’s Trophy and Iron Dome, many states are developing weapons systems with varying levels of autonomous capacity. The use of such systems has generated a divergence of opinion amongst lawyers, policy makers and human rights activists. While proponents are of the view that the current legal framework can be adapted to AWS with some modifications, critics argue that it will pose a major threat to the underlying principles of laws of armed conflict (LOAC).

Accountability, the foundational principle of international criminal law is indispensable to ensure the efficacy of LOAC. This chapter will examine whether the autonomous nature of the weapons, that distances or removes the human factor in the decision-making process, poses a challenge to establishing individual criminal responsibility under international criminal law. The chapter will evaluate whether and to what extent the current accountability framework can be used to ascribe individual criminal responsibility for war crimes committed by AWS and will reflect on a possible need to rethink the framework.

THE QUESTION OF ACCOUNTABILITY

Individual criminal liability is the “unchallenged cornerstone of the entire edifice of international criminal law”, which seeks to enforce the principles of international

134 A defence weapon system, which automatically detects airborne threats such as anti-ship missiles.

135 A protection system, for armored fighting vehicles, which can intercept and destroy incoming missiles and rockets.

136 A system that can intercept and destroy short-range rockets and artillery shells.


humanitarian law. Although the principle has been around for centuries, the first treaty codification of it can be found in the Draft International Convention on the Laws and Customs of War, produced in the Brussels Conference on the Rules of Military Warfare in 1874. Subsequently it was also recognized in the Versailles Treaty of Peace. However, it was the Nuremberg Tribunal that held individuals accountable for violations of international humanitarian law for the first time, thereby creating a precedent. Shortly thereafter, it gained recognition as customary international law. Since then it has gained large-scale recognition and has been codified by various states and international organizations culminating in the codification of the Rome Statute and the subsequent establishment of the International Criminal Court. Although the enforcement mechanisms are far from perfect, the principle is indispensable to ensure effective enforcement of the laws of armed conflict. An absence of it would undermine the law and impunity would flourish.

AWS are those which once activated can select and engage targets without further human intervention, making them different from other conventional weapons and remotely operated drones. The autonomous feature not only makes it uniquely effective but also equally unpredictable, particularly when deployed in complex environments or in the event where it malfunctions. In the absence of human oversight, it poses the risk of targeting civilians or non-military objectives in violation of the principles of international humanitarian law. This could result in what would be classified as war crimes if it were to be committed by a human. Autonomous weapons are abstract entities irrespective of their levels of sophistication and the Nuremberg Tribunal has specifically laid down that crimes are to be committed by men and not by abstract entities. This sets aside the


143 G.A. Res. 95 (1), Affirmation of the Principles of International Law recognized by the Charter of the Nuremberg Tribunal (Dec. 11, 1946).


145 Crootof, supra note 139, at 1360.

146 McFarland & McCormack, supra note 137, at 363.


148 Crootof, supra note 139, at 1349.

149 The Trial of the Major War Criminals Before the International Military Tribunal Nuremberg, Judgment, at 223 (Oct. 1, 1946).
possibility of ascribing individual criminal liability to autonomous weapons. Alternatively, even if they were to be given legal personality and held liable, they would not have satisfied the retribution and deterrence purposes that are part of the principle. Therefore it is only individuals who can be held accountable, but the absence of a human-in-the-loop raises the question of whether it amounts to a war crime and if yes, who can be held responsible for it. The “who” could be various humans associated with the AWS- the programmer, the manufacturer, the commander who ordered the use of the AWS in the particular context, or the soldier under whose watch the AWS acts in violation of international humanitarian law. Moving forward, we will examine how the accountability framework applies to AWS.

**LIABILITY REGIME**

Under international\(^{150}\) and domestic law\(^{151}\) regimes, mental element, in addition to actus reus, is considered crucial for ascribing individual criminal liability. Under the Rome Statute, a person can be held liable for grave breaches of international humanitarian law provided the willfulness element is established:

1. *Unless otherwise provided, a person shall be criminally responsible and liable for punishment for a crime within the jurisdiction of the court only if the material elements are committed with **intent and knowledge**.*

2. *For the purposes of this article a person has intent where:*
   a) *In relation to a conduct, that person means to engage in the conduct;*
   b) *In relation to a consequence, the person means to cause that consequence or is aware that it will occur in the ordinary course of events.*

3. *For the purpose of this article, “knowledge” means awareness that a circumstance exists or a consequence will occur in the ordinary course of events. “Know” and “knowingly” shall be construed accordingly.*\(^{152}\)

a) Direct Liability

Under international criminal law, an individual can be held liable for the war crimes he commits or is directly involved in, be it through planning or ordering of the act, provided he acted willfully.\(^{153}\) When it comes to an AWS, given the requirement of willfulness, no one can be held directly liable for its independent and unpredictable actions.

As AWS is an abstract entity, the element of mens rea cannot be established in its actions ruling out the possibility of ascribing it with accountability. In the instance where the

---


system is intentionally programmed or manufactured to commit a criminal act, the developer’s or manufacturer’s direct liability can be easily established. Similarly, a commander can be held directly responsible if – a) he either intended or foresaw the likelihood of civilian harm, despite which he employed the AWS, b) he intentionally ordered the use of AWS for the unlawful act. Here, the authority exercised by the commander can be either de facto or de jure and the mens rea need not be explicit; it can be inferred from the circumstances. However, in those instances where an AWS acts on its own devoid of any human intervention, willfulness component will not be present making it impossible to hold anyone directly liable for the crimes committed by it.

b) Indirect Liability

International criminal law provides doctrines that enable ascribing accountability to those who partake in war crimes despite not pulling the trigger by themselves. In short, the idea is to broadly cover all those who have partaken in war crime be it through omission or failure to perform their duty or assistance.

DOCTRINE OF COMMAND RESPONSIBILITY

Under this doctrine, military commanders can be held responsible for the criminal actions of their subordinates. This customary doctrine is premised on the idea that a superior can be held liable when he has failed to perform his duty to prevent his subordinate from committing a war crime. The Additional Protocol I, the ICTR statute, the ICTY statute and the Rome Statute have recognized and incorporated this liability regime. In fact, the ICTR and the ICTY played crucial roles in the development of the command responsibility doctrine through its various case laws. The main elements of this chargeable offence include

a) The occurrence of a crime within the jurisdiction of the ICC


155 Id.


157 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 86, June 8, 1977, 1125 U.N.T.S. 3

158 Statute of the International Criminal Tribunal for Rwanda art. 6(3), Nov. 8, 1994, 33 I.L.M. 1598

159 Updated Statute of the International Criminal Tribunal for the Former Yugoslavia art. 7(3), May 25, 1993, 32 I.L.M. 1192


161 Id.
b) The existence of a superior-subordinate relationship between the accused and the direct perpetrator of the crime
c) Exercise of effective control by the commander over the subordinate
d) Actual or constructive knowledge about the subordinate committing or about to commit the crime
e) Failure to take all necessary and reasonable measures to prevent or repress the crime or to report the matter

Therefore, primarily, to establish liability under the doctrine of indirect command responsibility, the subordinate should commit a crime covered under the Rome Statute. As discussed previously, “willfulness” is an indispensable element for establishing liability and since the subordinate in the context is the AWS, which acts devoid of the mental element, it’s action would not amount to a war crime. Furthermore, addressing the element of an existence of a superior-subordinate relationship, to date it has been held as an interpersonal relationship and therefore cannot currently be established in the case of an AWS.

One of the crucial components of the doctrine of command responsibility is that the commander should have effective control over his subordinate i.e. they should have the ability to “prevent or punish the criminal conduct”. In short, they should be able to oversee the actions of their subordinate and take necessary precautions to prevent him from undertaking any action in violation of the LOAC including the power to call off the action if required. However, in the case of AWS, even if the commander is engaged in real time monitoring of the system it would be impossible to exercise effective control over it. In light of its fast processing speed and ability to learn from the environment and adapt accordingly, the very purpose for which it is created, it can not only operate in an unpredictable manner but can also deprive the commander the power to prevent the criminal conduct. Therefore it is impossible to establish the existence of effective control over the AWS by the commander.

The doctrine also requires the commanders to have actual or constructive knowledge about the subordinate’s actions. In the case of AWS, actual knowledge can only be established if it were to communicate to the commander who its target will be prior to the attack. Furthermore, considering the complex nature of the algorithms that run the autonomous weapons, it would be difficult for a commander to foresee the actions that would be taken by it. In addition to this, the environment in which the AWS is deployed will also largely influence the manner in which it acts, making it difficult to predict its

---


165 FN 224 CR1
actions. As a consequence, even if there is real time monitoring, it would be difficult to establish that the commander had sufficient knowledge or time to call off the action. In the absence of actual knowledge, the next available option would be to establish that the commander had constructive knowledge or in other words if he had reasons to know of the likelihood of violation. The ICTY has held that such knowledge can be established if the commander had information that gave him “notice of the risk” of the subordinate’s actions which is alarming enough to “justify further inquiry” on it. However, in the case of AWS, it is unclear what information would satisfy the threshold of sufficiently alarming information, which would notify the commander of the risks posed by the AWS in question. Would knowledge of the past crimes committed by the AWS in question or any other AWS of the same making be sufficient? Should knowledge of a particular crime committed by the AWS put the commander on notice of all other possible types of crimes that can be committed by the AWS? Does the threshold vary depending upon the commander’s individual understanding of technicalities of the AWS? Therefore, without further clarity, it is difficult to determine what information can objectively be imputed to the commander to satisfy the requirement of constructive knowledge. Similarly, the final element- “all necessary and reasonable measures”- also warrants further clarity on what actions would amount to it.

In short, it can be said that the elements of command responsibility cannot be established in a situation where an AWS’s actions result in tragic consequences but devoid of the willful actions of a human. This could mean the possibility of an unnerving situation wherein a legal loophole is created vesting commanders with the power to use force through AWS without having the risk of being charged with individual criminal responsibility.

**Why not a Criminal Negligence Standard?**

Assuming a scenario in which an AWS malfunctions resulting in the death of civilians, the question arises as to if the commander who decided to deploy the AWS can be held liable. Some argue that the mere fact that the AWS can be unpredictable is sufficient to put the commander on notice of the risk. However such an argument is akin to saying that the commander should always be on notice of the possibility of a human soldier committing

---


169 Watch, supra note 166.

170 *Id*.

171 Beard, supra note 168, at 657.
an unlawful act.\textsuperscript{172} This boils down to creating a criminal negligence standard. If it is to be applied, in all those scenarios where a human soldier, or in this case AWS, goes rogue which could not have been reasonably foreseen by the commander, he would still be held liable. However this would be in contradiction to the moral principle underlying the criminal law regime.\textsuperscript{173} Mens rea, as we discussed is indispensable to establish liability. The International Criminal Court is also seen to disregard the concept of criminal negligence while upholding the higher threshold of “intent and knowledge”.\textsuperscript{174}

Incorporation of criminal negligence within the framework would pave the way for over criminalization, driven largely by politics, undermining the whole of international criminal law.\textsuperscript{175} Merely because we cannot hold anyone liable for the machine’s malfunctions does not automatically legitimize stretching the concept of dolus eventualis\textsuperscript{176} to the extent that we blindfold ourselves to the crucial element of individual guilt and the criminal law regime for our selfish interest.

**DEVELOPER ACCOUNTABILITY: A POSSIBILITY?**

The autonomous feature which makes the AWS different from other conventional weapons “extends to instigation of an action and not just performance”.\textsuperscript{177} Such actions are enabled by the software which runs it, which takes us to the next question pertaining to the legal accountability revolving around AWS: can the developers of these software be held accountable under international criminal law for the criminal outcomes of the AWS’s actions?

For the LOAC to apply, it is axiomatic that there should be an armed conflict, be it international or non-international. Therefore a war crime does not take place unless it’s committed within the context of an armed conflict. The Elements of Crimes document,\textsuperscript{178} which enumerates the elements of each of the crimes covered under the Rome Statute,


\textsuperscript{173} Crootof, *supra* note 139, at 1384.


\textsuperscript{175} Crootof, *supra* note 139, at 1384.

\textsuperscript{176} A form of intent in which the accused foresees the prohibited result not as one flowing directly from his act but as possibility and yet decided to proceed; See Kayitana Evode, *The Form of Intention Known as Dolus Eventalis in Criminal Law*, SSRN (July 31, 2008), https://ssrn.com/abstract=1191502.

\textsuperscript{177} McFarland & McCormack, *supra* note 137, at 368.

mandates the existence of an armed conflict for the commission of a war crime. In the case of software developers, it is therefore necessary that they develop the software controlling the AWS in the context of an armed conflict. However in most cases, the AWS would have been developed long before the armed conflict came into existence. Therefore the conduct in question is often divorced from the context of an armed conflict. The impossibility to satisfy this requirement could provide de facto immunity to the developers from war crimes committed by the AWS.

The most plausible ground for developer accountability is Ar.25(3)(c) of the Rome Statute which proscribes aiding, abetting or providing assistance in the commission or attempted commission of the crime. The Prosecutor could come up with the novel argument that “the culmination of acts perpetrated prior to the commencement of an armed conflict in the subsequent context of an armed conflict” is sufficient to satisfy the element. However there is no certainty as to whether it would succeed. The critical question here is whether such acts can occur prior to the commencement of the armed conflict. The Appeals Chamber of ICTY in its obiter dicta in the Blaškić judgment stated that the acts of aiding and abetting of a crime could occur before, during, or after the perpetration of the principal offence. This was further affirmed by the Trial Chamber of Special Court for Sierra Leone in Prosecutor v. Taylor. However in the former case the acts of the accused were not ex ante to the conflict and in the latter case, the acts in question were committed throughout the conflict. Therefore in the absence of jurisprudence establishing individual criminal liability for ex ante acts, it would not be possible to ascribe accountability to a developer.

Additionally, there is the obstacle of establishing the mens rea of a developer. If a developer builds the system such that it is incapable of distinguishing between civilians and military personnel, the mental element can be established with ease. However, in the hard case scenario where the system does not have such illegal features, the fact that the developer’s actions in question took place ex ante will serve as a barrier to establishing the mental element. According to the current jurisprudence, the accused should be aware of the criminal intent of the perpetrator at the time he commits the act that aids or abets the perpetrator in the commission of the war crime. Nothing suggests extending the mens rea element to cover the developer’s expectation that his work would provide assistance to a perpetrator who might form the criminal intent to use it in the future.

---


180 McFarland & McCormack, supra note 137, at 383.

181 Id.


183 See Prosecutor v. Taylor, Case No. SCSL-03-01-T, Judgment, ¶ 484 (May 18, 2012).

184 McFarland & McCormack, supra note 137, at 379.

185 Id. at 380.
Furthermore, in accordance with Ar.30 of the Rome statute, the Prosecutor has to prove that the developer acted with the intention to facilitate the commission of the crime. Therefore if the developer developed the software with the sole aim of selling it for profit, if we are to go by the literal interpretation of the statute, they cannot be held liable even if they were aware of the physical perpetrator’s intention and had knowledge that his product could assist him in the perpetration of the offence.  

To further complicate the issue, multiple organizations and individuals are involved in the development of complex weapons like the AWS, thus making it difficult to attribute the responsibility for a flaw to a particular individual.  

The Rome statute specifically states that the definition of a crime has to be construed strictly and that if ambiguity arises, it has to be interpreted in favor of the accused. Such a stance combined with the absence of jurisprudence regulating ex ante conduct, renders it impossible to satisfy the elements of war crime within the current framework to ascribe individual criminal responsibility to an AWS developer. 

Therefore international criminal law in its current form is an imperfect framework to establish accountability for violations of international humanitarian law stemming from the use of AWS. However the accountability gap does not mean that the possibility of amending or reforming the law to apply it to a context in which AWS is used is out of question. To start off, the requirement that the acts in question should occur within the context of an armed conflict or the requirement of mens rea could be amended in such a manner that it would bring under its ambit ex ante actions discussed above. Therefore we should not discard the possibility of establishing individual criminal responsibility with respect to AWS. Joint and concerted efforts from the states and relevant actors can bring about desired results that could help in striking a balance between the interest of both the proponents and opponents of the AWS.  

**THE WAY FORWARD 1.0: DYNAMIC DILIGENCE** 

To adequately address the challenges posed by AWS to the accountability framework, Prof. Peter Margulies proposes what is called a “dynamic diligence” approach that hinges on the doctrine of command responsibility. He proposes holding commanders in power accountable for violations of LOAC committed by AWS but with a slight modification to the

---


187 McFarland & McCormack, supra note 137, at 381.


current framework. His model incorporates an active, engaged and informed role for the commanders.

The approach entails three prongs: a human-machine interface; dynamic assessment, and dynamic parameter, all tailored to ensure AWS’s compliance with international humanitarian law. The human-machine interface is premised on a dedicated AWS command structure comprising of commanders and staff with machine learning skills and technical expertise. Although the model does not propose human ex ante supervision of the AWS’s targeting process in all cases, it suggests an adaptable interface that calls for human intervention depending upon the complexities of the environment in which it is deployed along with the option to override the machine learning protocol if required. Such an approach is in line with the arguments of proponents of AWS who argue that ex ante human intervention would interfere with efficiency in targeting, especially when time is of essence.

Dynamic assessment entails what we would expect a commander to do when he engages with his human subordinates, except in the case of AWS his tasks would be more technical in nature. It requires commanders to do regular reviews of the machine's learning process including running tests on the AWS to ensure that it works in compliance with the principles of distinction and proportionality enumerated in the international humanitarian law and modifying software in case of non-compliance. It also includes the task of ensuring that the evidence relied on by the AWS such as the terrorist watch lists are updated regularly so that there is no scope for false positives when it comes to automated targeting.

Dynamic parameters, the final prong, proposes limits on various parameters such as time, distance and maximum collateral damage so as to reduce the chances of the AWS going rogue, and also to reduce the damages in the unfortunate event it does. It suggests setting default time and distance limits, exceeding which the AWS should go into hibernation mode with the possibility to override it through human intervention. The idea behind setting a limit on the collateral damage is to ensure that targeting decisions of the AWS are in compliance with the proportionality principle. Furthermore it proposes greater transparency on the targeting decisions.

The dynamic diligence approach, with its three prongs, ensures “meaningful control” such that it does not interfere with the autonomy of the weapons but at the same time it keeps a check on it by bringing a human-in-the-loop. A modest revision of the command responsibility doctrine along this pattern could help in alleviating the concerns of the accountability gap created by the use of AWS while ensuring compliance with the international humanitarian law principles.

---

190 See Id. at 19-21.

191 See Id. at 21, 22.

192 See Id. at 22-214.
THE WAY FORWARD 2.0: WAR TORTS AND DYNAMIC DUE DILIGENCE

The current debates around AWS focus only on the issue of the accountability gap created by it in the existing framework of international criminal law. However we should not forget that there is more to accountability than just individual criminal liability. State responsibility is also an equally important factor that needs crucial discussion in the context of AWS. There is already a framework in place that holds states accountable for “internationally wrongful acts” provided the conduct in question is attributable to the state. This includes even serious violations of international humanitarian law. However with the advent of international criminal law, a special term – war crime- came into place establishing individual criminal liability along with it. But state accountability and individual criminal liability are not mutually exclusive. Therefore, at least until the accountability gap in the current international criminal law framework is resolved, we should focus on holding states accountable for the wrongs committed by the AWS so as to enforce the principles of international humanitarian law. In fact, holding states accountable seems more practical as they are not only in a better position to ensure that the AWS is designed and employed in compliance with the principles of international humanitarian law but also because a duty to ensure the same is vested on them by Additional Protocol I.

Rebecca Crotoof, in a seminal article, proposes a novel concept of “war torts” to enforce state accountability for serious violations of international humanitarian law. This could be a very useful approach because although the purpose of both criminal and tort laws are to deter crimes and uphold accountability for such actions, each regime deals with two different kinds of actions. While the former focuses on moral wrongs the latter focus on injurious wrongs including unintended ones. Therefore establishing a “war torts” regime would in no way undermine the international criminal law regime. In fact, it could


197 See Crotoof, supra note 139, at 1386-1393.

198 Laura, supra note 156, at 92.
aid in establishing accountability for some of the harms that could potentially arise from the use of AWS but are left unaddressed by the criminal law regime. 199 Thus, a war torts regime would help in reinstating a state’s responsibility specifically with respect to war crimes. Furthermore, attribution of the AWS’s actions to the state brings an additional benefit to the victims in the form of reparations, which is not provided for under criminal law. 200 Also, since it’s the state that takes the call on developing, purchasing or integrating AWS into their warfare system, ascribing accountability for its wrongful actions to the state has higher chances of serving as an effective deterrent to prevent its overuse rather than individual criminal liability. 201

Adopting a “war torts” regime for regulating AWS comes with the question of what level of liability should it incorporate. Considering the autonomous nature of these weapons, which makes them unpredictable, it will most likely be difficult to establish absence of due care. 202 The issue is made further complicated by the involvement of a large number of individuals in the development of sophisticated AWS which makes it difficult to trace the causal chain of injuries. 203 All these factors make it impossible to establish liability under negligence standard. The strict liability standard is often employed to deal with cases involving lawful but inherently dangerous activities. 204 There is no denial of the fact that the autonomous nature of the AWS makes it not only unpredictable but inherently dangerous as well, since not only can it go rogue despite exercising due care but in the event it does it affects human lives. 205 Therefore a strict liability standard, as proposed by Crootof, seems appropriate to deal with AWS. A war torts regime also calls for an independent tribunal, much like the other specialized tribunals that we have in place to adjudicate on it, as holding a foreign state liable for international crimes in domestic courts could come with a myriad of political problems.

Although state responsibility does not replace individual criminal responsibility for war crimes committed by AWS, it appears to be a plausible approach to address the accountability gap for the time being. In fact, as rethinking of the current international criminal law regime would be a time consuming process due to the divided stances on AWS, an absence of state responsibility would result in an unregulated situation, which could wreak havoc. Moreover, as both can exist in conjunction with each other, upholding

199 Id.
201 André Nollkaemper, System Criminality in International Law 1, 4 (Harmen van der Wilt & André Nollkaemper eds., 2009)
202 Crootof, supra note 139, at 1385.
203 McFarland & McCormack, supra note 137, at 384.
205 Crootof, supra note 139, at 1385.
206 Id. at 1399.
the former would in no way hinder the development of the latter (to suit AWS) in the future.

WHAT IS THE WAY FORWARD FOR INDIA?

The legal and ethical questions around AWS are a long way from answered. However the delay in the deliberations is unlikely to affect their development and proliferation. Therefore India has to adopt a strategy to deal with the issue at hand until a global consensus is reached. The urgency is further exacerbated by the fact that it is located in a complicated geopolitical context, with its neighboring states China already focusing on AI led military innovation. Additionally, while Pakistan has demanded a preventive prohibition of AWS, its previous history regarding nuclear weapons wherein it called for a nuclear-free South Asia while simultaneously developing nuclear weapons, makes it impossible to take it at face value.

At the forum for Convention on Certain Conventional Weapons (CCW), India emphasized on the need to ensure that the resort to AWS in battlefields in the name of lesser casualties is not encouraged. However, recognizing the possibility for a rise in technology gap between states, it does not support an outright ban but suggests the adoption of a strategy that strikes a balance between the lethality and military necessity of these weapon systems. In fact, it has been expressing a willingness and intent to develop autonomous weapons by increasingly adopting AI and other modern technologies in its defence sector. Since the 1990s, giving predominance to national security concerns, India has been supporting pragmatic arms control treaties. This is

---


211 Id.

212 Mohanty, supra note 208.


evidenced by the fact that it has not become a party to the Ottawa Treaty.\textsuperscript{215} Therefore, India signing a treaty that bans the development of AWS is highly unlikely, especially considering that it could ensure a strong military edge over its adversaries. However it could be a cause for concern for the international community as India has not ratified Additional Protocol I to the Geneva Conventions,\textsuperscript{216} despite having ratified the latter. Ar.36 of the AP I require states to conduct a legal review of any new weapon before it is used in warfare. Absence of such a review process would fail to ensure the compliance of the AWS with the underlying principles of IHL, which could lead to fatal consequences. It is further complicated by the fact that India is not a party to the Rome Statute.\textsuperscript{217} One of the major reasons for India’s reluctance is its desire to avoid the possibility of its military personnel being indicted in a foreign state by “an over zealous or politically motivated ICC prosecutor” for an alleged crime committed during the course of their duty.\textsuperscript{218} Such an approach further heightens the risk while employing AWS since in the absence of Rome Statute (in the event it is modified to fill the current accountability gap posed by AWS) establishing individual criminal liability would be impossible.

An international framework on the use of AWS is therefore quintessential. From India’s perspective, AWS provides it with military benefits in the form of effective patrolling of its borders and reduced casualties,\textsuperscript{219} while at the same time having the potential to be misused by states as well non-state actors. Therefore, it is in its interest to actively contribute towards the debate to develop a pragmatic global regulatory mechanism on the development, use and trade of such weapons.\textsuperscript{220} While it remains to see whether India would actually deploy AWS, as one of the states involved in developing it, it could come up with a domestic strategy to address these concerns. This could involve a domestic legal framework\textsuperscript{221} that establishes liability for the actions of AWS, in the form of a dynamic diligence requirement or a war torts regime, and lays down the rules of conduct. As the international conversation on AWS is still at a nascent stage, this could serve as the framework for an international regulatory mechanism.


\textsuperscript{218} Dilip Lahiri, Should India Continue to Stay Out of ICC?, OBSERVER RESEARCH FOUNDATION (Nov.24, 2010), https://www.orfonline.org/research/should-india-continue-to-stay-out-of-icc/.

\textsuperscript{219} REDDY, supra note 209, at 10.

\textsuperscript{220} Id. at 13.

\textsuperscript{221} Id. at 14.
CONCLUSION

Of all the challenges posed by AWS to international humanitarian law, perhaps the most daunting and complex one is that of accountability. International criminal law, in its current framework is toothless, when no individual acts willfully, which is precisely the case here. But absence of individual criminal responsibility does not automatically make the AWS unlawful or warrants its prohibition.\(^{222}\) The legality of a weapon system is not determined by whether an individual can be held liable for its criminal actions. It is often the case that technologies develop at a rapid pace resulting in a growing gap between emerging technologies and legal regimes. However as the circumstances on the ground changes, the law should also evolve simultaneously. Given that AWS is here to stay, and in light of the fact that a ban of it could even have potential detrimental effects as AWS come with the benefits of greater precision and reduced military casualties, we should try to develop an alternative accountability regime that could be effective in its case. However, time is of essence here. Unless immediate action is taken, be it in the form of a dynamic diligence approach or of war torts regime or a tailoring of the current framework to suit the AWS, states might get entangled in an AWS race, which could have significant and irreversible effects undermining “hard-won humanitarian protections”.\(^{223}\)


\(^{223}\) See Crootof, supra note 147, at 1894-96.
CHAPTER 4: AUTONOMOUS WEAPONS SYSTEMS AND THE PRIVATE SECTOR

Elizabeth Dominic

INTRODUCTION

With the rapid advancements in technology and its increasing penetration into our daily routines, the tech sector, dominated mostly by private entities, has come to the forefront in all domains. Traditionally, the military industry used to be the brain behind most of the technological innovations, which it later used to cater to the civilians resulting in a “spin-off” effect. However, currently what we witness is a reversed pattern wherein the private sector innovations are “spun-in” to the defence sector. While Internet and GPS were developed in The Defence Advanced Research Projects Agency (DARPA) funded labs, emerging technologies of today are developed in Google and other big tech companies.

The private sector with its human capital, research and development, and infrastructure has become the dominant developer of all novel technological innovations including autonomous ones with the aid of Artificial Intelligence (AI) and Machine Learning (ML), the brainchildren of Big Tech. The military is therefore increasingly relying on the private sector to meet its immediate needs to develop autonomous weapons. This means, AI that has been developed with the goal of aiding civilians in numerous ways—from controlling traffic to providing assistance in healthcare—is now being tailored for military applications. So there is an increasing trend of tie-ups between the defence departments and private tech sector.

WHAT’S THE BIG DEAL?

Many key tech companies are actively developing technologies with the goal of enhancing human living standards. However most often they have dual purposes and that’s where


the problem begins. For instance, automation, AI, and face recognition technologies have the potential to be repurposed for the military. In the case of AWS, these technologies can be used to gather and process large amounts of raw intelligence information so as to identify targets. They can also be incorporated within the weapons themselves to execute missions. This is already being utilized in Project Maven where AI is used to interpret video images to facilitate identification of targets. Thus even if a company is not actively involved in the process of developing AWS, it can still effectively contribute towards it if its technology can be used for the same. Therefore in the absence of clear policies that explicitly prescribe the purposes for which the technology can be used and proscribe others, there is always the risk of their technology aiding the development of AWS, which can potentially pose a major threat to humanity.

A LOOK AROUND THE WORLD

Many states are increasingly investing in exploiting AI in a new domain, military, particularly with the goal of developing AWS. They are engaged in a race to outpace their adversaries, leaving others with no option but to follow suit. This is pointing us in the direction of an AI arms race, akin to the nuclear arms race of the 20th century. Despite the risk it poses to humanity, development of such weapon systems in stages is proliferating at a fast pace.

USA, a key player in this field, is committed to exploiting the developments in AI and autonomy within their military technology. The Advanced Targeting and Lethality Automated System (ATLAS) program that aims to use AI and ML to enable autonomous target selection within ground-combat vehicles is an indication of it. In response to the shift in the innovation landscape, the Pentagon is increasingly involved in private sector engagements. In fact, the state has been making significant strides towards development of AWS by collaborating with powerful tech companies such as Microsoft, Amazon, and Clarifai, despite Google pulling out of Project Maven. The Defence Innovation Unit set up in Silicon Valley is also part of the initiatives to further the public-private partnerships to strengthen the military technologies. It serves as a “liaison between the Defence

228 Id. at 3.


230 See PAX, Don’t Be Evil (2019).


232 PAX, supra note 207, at 4.


234 PAX, supra note 230, at 4.
Many of the tech companies, guided by profit motives, are more than willing to extend aid to the military to develop lethal weapons, often arguing that without their help the defence department would be in a crisis as other countries are also engaged in a similar AI race. These practices indicate how much has changed since a few years when the idea of killer robots was considered an anathema.

China, another dominant player, in the 2018 UN GGE on lethal autonomous weapon systems, expressed its interest to “negotiate and conclude” a new protocol to ban the use of fully autonomous lethal weapon systems. It’s interesting to note that their support of a ban was confined only to the “use” and not to the “development” of such weapons, which raises questions about the state’s exact stance on the issue. As a large amount of the AI research in China is being undertaken in private tech organizations, the government is seen to be increasingly relying upon them. Following the American model of defence industry, China has adopted a “civil-military fusion” to bolster the development of dual use technologies in various industries including automation and information technology and thereby to further the participation of private tech companies in the state’s defence related activities. However, interestingly, chairman of Alibaba, the leading Chinese multinational technology company, has raised concerns regarding the use of AI and ML by the military and its potential to result in yet another World War. Despite such concerns raised by the private sector, the Chinese military is actively incorporating AI in its weapon systems.

---


236 PAX, supra note 230, at 14.


238 Id.

239 PAX, supra note 207, at 14.


241 PAX, supra note 207, at 13.
Israel, one of the most technologically advanced military states, strongly opposes an international treaty banning the use of AWS. The Israeli military already employs weapons with autonomy, Harpy loitering munition being one of them. In Israel, public-private partnerships, particularly between the military and the digital sector, is a common practice in the development of military technologies. Considering how advanced the state is in its AI research and development, it won’t be long before it develops and employs AWS within its military.

South Korea, despite acknowledging the risks that could be posed by autonomous weapons that remove meaningful human control from its operation, is a strong advocate for the AWS for defence purposes. Similar to Israel, South Korea is yet another country that is advanced in the development of weapons with considerable autonomy. It is already using SGR-A1, a sentry robot, with the ability to identify intruders and fire at them without any human intervention, developed by Samsung Techwin and Korea University, in the Korean demilitarized zone. Public-private partnership is an integral component of the Korean military strategy, and it is increasingly collaborating with local universities and research entities to further AI research.

**WHERE DOES INDIA STAND?**

India, while leading the debate on AWS at the UN GGE did not endorse a ban. Recognizing that states are rapidly gearing up for a new AI driven arms race, India is keen on catching up. Its interest in AWS could also be driven by its precarious security situation with two hostile neighbors and the looming threat of insurgency.

---


244 It is an anti-radiation drone, which can either operate fully autonomously or have a human-in-the-loop, designed to loiter the battlefield and to attack radar systems by self-destructing into them.

245 PAX, supra note 207, at 28.

246 Gronlund, supra note 231.


248 PAX, supra note 207, at 32.

249 Mohanty, supra note 208.

India is already using semi-autonomous weapon systems such as the Phalanx Close-IN Weapon System \textsuperscript{251} and Muntra \textsuperscript{252} that targets objects. It indicates India’s readiness towards adopting weapons with greater autonomy. In fact, in anticipation of an AI driven futuristic warfare, the Defence Research and Development Organization (DRDO) is currently developing robotic soldiers, with the potential to work like human soldiers, to boost its unmanned fighting capacity. \textsuperscript{253} Its description is very similar to that of a fully autonomous weapon system as it is claimed that they would have a “very high level of intelligence to enable them to differentiate between a threat and a friend.” \textsuperscript{254}

As India embarks on the road to upgrading its defence equipment with modern technologies, it plans on developing at least 25 AI related weapon systems in the next five years. \textsuperscript{255} It has set up a multi-stakeholder task force headed by Tata Sons Chairman N. Chandrasekaran, comprising of members from academia, industry, government, and startups to spearhead the AI projects. \textsuperscript{256} One of the major goals of the task force is to develop “potential transformative weaponry” including autonomous robots. \textsuperscript{257} Although, currently, India might not have the likes of Google and Amazon, its IT and software sector is well advanced. Indian technology giants such as Infosys and Tata have in fact made significant strides in AI and robotics technologies. \textsuperscript{258} Recognizing the strength of the sector, the government is trying to establish cooperative partnerships between the Indian private sector and the global Original Equipment Manufacturers (OEMs) to facilitate “technology transfers” and to “set up domestic manufacturing infrastructure and supply chains.” \textsuperscript{259} Furthermore, with the aim of boosting the indigenous capabilities, the government in collaboration with MSMEs, startups, and academic institutes is planning to set up defence innovation hubs across the state focusing on futuristic technologies such as AI, quantum, cognitive, and asymmetric technologies, and smart materials. \textsuperscript{260}

\begin{thebibliography}{99}
\bibitem{Gupta2020} Palak Gupta, Hi-Tech Defenders, Force, \url{http://forceindia.net/feature-report/hitech-defenders/} (last visited May 20, 2020)
\bibitem{IndiaToday} India Today, supra note 82.
\bibitem{Id} Id.
\bibitem{Chawla2020} Vishal Chawla, AI-Based Defence Technologies Are Hot At India DefExpo 2020, AIM (Feb.6, 2020), \url{https://analyticsindiamag.com/ai-based-defence-technologies-are-hot-at-india-defexpo-2020/}.
\bibitem{Id} Id.
\bibitem{Mohanty} Mohanty, supra note 250, at 6.
\bibitem{Chawla} Chawla, supra note 255.
\end{thebibliography}
These developments indicate India’s intention to transform from a major arms importer state to an arms exporter state with the aid of the private technology sector. Towards this, India has set a target of $5 billion worth of military exports in the next 5 years and is inviting global defence majors to set up their manufacturing units in India.\textsuperscript{261} At the DefExpo 2020, Defence Minister Rajnath Singh hinted at the possibility of a new partnership between India and South Korea, in developing AI enabled weapon systems, while identifying the defence corridors as an ideal platform for the South Korea industries to set up their manufacturing units.

India, therefore, in anticipation of an AI led warfare has initiated active efforts in incorporating AI and other modern technologies in its defence sector. Realizing the crucial role of the tech sector in this venture, it is adopting measures to enhance cooperation with it. The latter also appears to be extremely keen on fostering the partnership as is evident from the large number of Indian companies that took part in the DefExpo 2020.\textsuperscript{262} In light of India’s technology prowess, such partnership would aid the state in making great advancements in the development of AWS.

**The Divided Stance**

Off late, much debate has been going on within the tech sector regarding the acceptable and non-acceptable uses of AI, the increasing use of adaptation of automation technologies within the weapon systems being one of them. The stance that the tech companies have adopted on the issue appears to be divided. Clearpath Robotics, a Canadian company having a history of involvement with military research and development, recognizing the fatal nature of AWS, was the first company to adopt a firm stand against the manufacturing of AWS.\textsuperscript{263} Similarly, in 2018, Google met with protests from its employees urging it to revoke its contract with the Department of Defence in Project Maven for fear that the technology could be used in the future to develop AWS.\textsuperscript{264} Consequently, Google not only ceased its involvement in the project but also adopted a policy declaring its commitment to not partake in the development or use of AI for weapon systems or other technologies that could prove to be fatal for human lives.\textsuperscript{265} It

\footnotesize{\textsuperscript{261} CHAWLA, supra note 255.}

\footnotesize{\textsuperscript{262} ASHOK, supra note 252.}


\footnotesize{\textsuperscript{265} GOOGLE, Artificial Intelligence at Google: Our AI Principles, https://ai.google/principles (last visited May 4, 2020).}
was immediately followed by a pledge by over 240 companies and 3200 individuals, including powerful technologists like Elon Musk and Mustafa Suleyman to never participate nor support the development and use of lethal autonomous weapons.

To the contrary, various Big Tech companies- Microsoft, Amazon, IBM, and Oracle- were bidding for the US Defence Department’s Joint Enterprise Defence Infrastructure (JEDI) Programme, with Microsoft beating Amazon in the final bid. The objective of the programme as explicitly stated is to “enhance the lethality of the department”. Microsoft has also entered into a contract with the Pentagon to provide it with Hololens, which again is explicitly stated to be used for the purpose of enhancing the lethality. Both the projects have met with widespread opposition from the employees. Despite its publication “Future Computed” in which it emphasized on the importance of having ethical principles in place to keep a check on the use of AI, the company has continued to engage with the military projects without any such policy in place. Interestingly, it’s the very same company that has been at the forefront advocating for Digital Geneva convention. These companies justify their action on the grounds that such support is quintessential to making the defence department stronger. Although such tie-ups are not intrinsically problematic, they at the same time must ensure that their technology is not put to use for unethical and lethal purposes.

A recent report by Pax, a Dutch group that is a part of the “Campaign to Stop Killer Robots” initiative further evidences this. It conducted a survey of 50 companies in 12 states, regarding their involvement and policies concerning AWS and classified them on the basis of three criteria:

“1) Is the company developing technology that could be relevant in the context of lethal autonomous weapons?”

---

266 PAX, Supra note 230, at 4,7.


270 PAX, supra note 230, at 16.


2) Does the company work on relevant military projects?
3) Has the company committed to not contribute to the development of lethal autonomous weapons?²⁷³

Based on the analysis it identified 7 companies having the “best practice” in place in light of their strong commitment to ensure that their technology won’t be utilized for the manufacturing of AWS, with Google being one of them.²⁷⁴ 22 companies were identified as of “medium concern” due to the fact that they do not have a policy in place proscribing the use of their technology for the development of AWS although they are not currently involved in such projects.²⁷⁵ 21 companies were identified as of “high concern”, Microsoft, Amazon, and Oracle being few of them, in light of the fact they develop technologies of interest to the military and are already engaged in various military projects despite not having policies prohibiting the use of technologies in AWS.²⁷⁶ The fact that some of the most powerful and influential tech companies are identified in the category of “high concern” is extremely disturbing and calls for an immediate action to restrict the development of and use of AWS.

WHAT CAN THE PRIVATE SECTOR DO?

Technology has the potential to do good to society but if not used for the right purpose it can have huge repercussions. AWS developed with the aid of advanced technologies raises concerns in many fronts-ethical, legal, and security. Many leading technologists have termed it as the third revolution in warfare.²⁷⁷

As we have seen, tech companies play a crucial role in the development of AWS with the increasing reliance of the defence departments on them to tailor their technologies for the former’s interests. However, the tech companies have a social responsibility to ensure that their developments are used for the benefit of humanity and not to the contrary. They should not let short-term monetary profits override their social goals. Yet most of them have demonstrated limited willingness to ensure the same.

Tech companies should recognize the pertinent role they play in the debate and must take measures to ensure that their technologies do not contribute towards the development of AWS. In fact, failure to do so can result in huge reputational costs and backlashes.²⁷⁸ Although many tech companies have policies on AI in place, most of them

²⁷³ PAX, supra note 230, at 4.
²⁷⁴ Id.
²⁷⁵ Id. at 4, 29.
²⁷⁶ Id. at 4.
²⁷⁷ Browne, supra note 240.
²⁷⁸ PAX, supra note 230, at 18.
do not address military application of it. However it is imminent for them to prioritize setting up concrete policies that explicitly state acceptable and non-acceptable military applications of their technology. Such a strategy is the only way to ensure that technology is used for the advantage of the military but not at the cost of human lives.

279 PAX, supra note 230, at 24.