Legal Preparedness and Governance of Ai-Driven Warfare: A Doctrinal Study on India's Legal and Strategic Readiness

AUTHOR:

V. AKSHARA SARADHA 126117003

CO-AUTHOR: SRIVIDHYA N 126117033

ABSTRACT:

The amalgamation of Artificial Intelligence (AI), autonomous weapon systems (AWS), and cyber capabilities is revolutionizing contemporary combat, reshaping doctrines of command, control, and accountability. India's defence modernization has progressively adopted these technologies to improve strategic deterrence and operational efficacy. Nonetheless, this swift acceptance has surpassed the evolution of appropriate legal and institutional protections. The lack of legal acknowledgement of AI-related harm, ambiguous liability criteria, and disjointed collaboration among cybersecurity, data protection, and AI governance frameworks has resulted in a regulatory void. This article does a doctrinal and comparative review of India's readiness to address AI-driven conflict, scrutinizing the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and pertinent to various international or foreign frameworks. India's capacity to guarantee accountability and adherence to international humanitarian law is compromised by significant legal and regulatory inadequacies, according to the study. In order to maintain accountability, openness, and the rule of law in the era of intelligent warfare, it closes by suggesting a single legal and institutional framework that integrates cyber governance, AI ethics, and defence policy.

KEYWORDS: Autonomous weapons System, Lethal Autonomous Weapon System, Warfare, Espionage, Cyber Governance, Department of Defence, Defence Acquisition Procedure, Drone, Surveillance, Conventional Munitions and Unmanned Aerial Vehicle.

INTRODUCTION:

The development of autonomous systems, cyber capabilities, and artificial intelligence (AI) has permanently changed how warfare and espionage are organized in the twenty-first century. The unseen but powerful domain of cyberspace, where information manipulation, digital surveillance, and cyber-espionage function as new tools of state power, is where modern conflict extends beyond conventional battlefields.

The increasing integration of technology into national defense highlights the need for an all- encompassing and forward-thinking legislative and institutional framework for India, a fast- modernizing country with significant geopolitical risk. The confluence of international law, technological innovation, and national security now necessitates readiness not only in infrastructure and innovation but also in cyber jurisprudence, accountability, and adherence to international humanitarian obligations. The Information Technology Act, 2000, which gives the Indian Computer Emergency Response Team (CERT-In) authority under Section 70B to advise intermediaries and businesses on cybersecurity and incident response, is the main foundation of India's existing cyber defense system[1].

The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013, which specify procedural requirements for reporting and mitigating cyber events, complement this. Furthermore, India's defensive foundation for cyberspace defense is comprised of frameworks like the National Cyber Security Policy (NCSP) and the National Critical Information Infrastructure defense Centre (NCIIPC) under the National Technical Research Organisation (NTRO). These tools, however, mainly deal with traditional cyberthreats and do not yet provide clear legal readiness for offensive cyber operations, AI-based autonomous warfare, or the intricacies of digital espionage carried out by state or non-state actors.

In parallel, through cooperation with start-ups, MSMEs, and research institutions, India's defense innovation ecosystem that is shaped by the Defence Acquisition Procedure (DAP) 2020 and the Innovations for Defence Excellence (iDEX) framework which has established the groundwork for technical self-reliance. This strategy aims to indigenize the development of cutting-edge military technology including artificial intelligence, robots, and autonomous systems in line with the government's Atmanirbhar Bharat vision. However, as AI-powered surveillance tools and autonomous weapon systems (AWS) develop, they present previously unheard-of ethical and legal issues with regard to accountability, proportionality, and adherence to the Convention on Certain Conventional Weapons (CCW), especially its protocols on Lethal Autonomous Weapons Systems (LAWS).

As a signatory to the CCW, India has backed the Group of Governmental Experts' (GGE) discussions, stressing the need to uphold the norms of International Humanitarian Law (IHL), such as distinction, precaution, and proportionality, and to maintain meaningful human control. Despite these initiatives, India does not have a single domestic legal framework that addresses algorithmic targeting, autonomous cyber operations, or digital espionage, which causes uncertainty in monitoring and enforcement. The country's cybersecurity response remains fragmented across agencies such as CERT-In, NCIIPC, the Defence Cyber Agency, and the National Cyber Coordination Centre (NCCC) where each initiatives address specific domains without an overarching legal harmonization[2].

Therefore, this research study critically examines India's legal readiness for espionage and digital warfare, assessing the suitability of its existing institutional structures, laws, and international obligations. In order to bring India's strategic, technological, and humanitarian goals into line with international norms of accountability and governance, it looks for legislative and structural gaps and suggests reforms.

RESEARCH PROBLEM:

The rapid integration of Artificial Intelligence (AI), autonomous systems, and cyber weapons into modern warfare has outpaced India's legal and institutional preparedness. Despite advancements in defence capability, there is no statutory framework defining accountability or liability for AI-driven military actions. Existing laws, including the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000, lack provisions to address algorithmic misconduct in warfare. Furthermore, poor inter-agency coordination weaken cyber and AI regulation.

RESEARCH OBJECTIVE:

This study specifically aims at the following perspectives:

1) Examine India's existing legal framework including the Information Technology Act, 2000

with respect to the meaning of the term Autonomous weapon system.

2) Analyse institutional mechanisms to evaluate their accountability within India's digital

defence framework.

3) Analyse how various countries legislative frameworks regulate the adoption of AI-driven weapons to guarantee attribution and accountability.

HISTORICAL BACKGROUND:

India has consistently faced concerns of cyberattacks from hostile neighbour states, such as China and Pakistan, which might harm essential infrastructure, important weapon platforms, and ISR (Intelligence, Surveillance, and Reconnaissance). The Convention on Certain Conventional Weapons (CCW), which was presided over in 2017 and 2018, has India as a signatory. A short film was shown at the United Nations Convention on Certain Conventional Weapons (CCW) meeting in Geneva in November 2017. Titled 'Slaughterbots', it showed a contractor advertising his latest product – a small drone with artificial intelligence that has the ability to find, target and kill. The film goes on to show the drones fall into the wrong hands, get unleashed onto the world and proceed to wreak havoc by

[1] https://www.cert-in.org.in/

[2] https://www.mea.gov.in/

indiscriminately shooting people in the head[3]. The convention declared eleven guiding principles on LAWS that were developed. India is assumed to obtain significance for building autonomous systems for national security by assessing its position in this convention. Under the protection of 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 (Convention on Certain Conventional Weapons or CCW), the group of Governmental Experts (GGE) convened a meeting on Lethal Autonomous Weapons Systems (LAWS). The Indian government has allocated orders for domestic micro, small, and medium-sized enterprises (MSMEs) up to INR 100 crore per year under the Defence Acquisition Procedure (DAP) 2020. There are 81 Innovations for Defence Excellence where an innovation ecosystem, was also founded in 2018 to support technological development and innovation in defense with start-ups, MSMEs, innovators, academia, and R&D institutes through grants and research funding.

However, emerging technologies are only disruptive to the extent that they will change the essence of war and they will increase the physical distance between adversaries, expedite its execution, and create new avenues for escalation and de-escalation.

The Department of Defense (DoD) in the United States has defined what an Autonomous weapon is, which, once activated, can help in engaging and mapping the targets without any further human intervention[4].

Several analysts have argued that the technology to be regulated is premature as it becomes impossible to predict how the autonomous weapon generated by AI will look like in the future. Indeed, Slaughterbots was dismissed by critics as an alarmist and exaggerated portrayal of the ‘killer robot’ technology that is popular in dystopian science fiction movies. From self-driving cars in the automotive industry to robot assisted surgery in healthcare, the adoption of increasingly sophisticated technology is being endorsed for reducing human error and increasing productivity and efficiency in almost every field. New forms of automation is increasing in autonomy to the technology of weapons to act independently without human inputs. A similar weapon was made by a South Korean Company which developed a lethal sentry robot that was used to identify targets in hostilities without any human intervention. The robot was named as “SGR-A1 Sentry Guard Robot[5].

These developments have already been noticed by India. Presently, India has set up a multi- stakeholder task force under the military of defence for the protection of national security and provided measures for both defensive and offensive AI in several places that includes aviation, naval, land systems, cyber and nuclear. The NITI Ayog has updated one National strategy on AI that targets on the goals of India which includes AI capabilities and navigating its path. Instead of India following the principles laid down under LAWS and running a rat race behind various developed nations with AI technologies, it can incorporate in a manner such that it is keeping a unique standard and experience for the part of global south.

The Central Government of India gave directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe and Trusted Internet, where sub- section (6) has been defined as, CERT-in was empowered to call for giving directions to the intermediaries and other corporate authorities for carrying out functions enshrined under the section of the IT Act, 2000. During emergency, various cyber security incidents such as Targeted scanning, compromise of critical information, unauthorised access, spyware and various other cyber thefts have been coordinated by the response team providing measures and primary information that are essential for carrying out the analysis, coordination and the investigation procedure in accordance with law. The date centre should also connect with the Network Time Protocol (NTP) Server of National Information Centre (NIC) or National Physical Laboratory (NPL) for integration of ICT system clocks[6].

Furthermore, the possibility of completely autonomous systems has sparked heated discussions in diplomatic channels, posing basic concerns about human dignity, responsibility, and the moral bounds of technical advancement in addition

[3] ibid

[4] U.S. Dep’t of Def., Directive 3000.09, Autonomy In Weapon Systems 13–14 (Nov. 2, 2012), available at <http://www.dtic.mil/whs/directives/corres/pdf/300009p.pdf> [hereinafter Dod Directive 3000.09].

[5] https://www.lawfaremedia.org/article/foreign-policy-essay-south-korean-sentry%E2%80%94-killer-robot- prevent-war

to the nature of future combat as India meets various unique challenges in the argument of LAWS. For security landscapes, India has to be legally prepared for crossroads of technological armed conflicts. This also includes taking measures at international forums, one such being International Humanitarian Law, safeguarding technological defence preparedness[7].

This paper brings out a clarification of India's approach towards the Defence Acquisition Procedure (DAP), 2020 for the establishment of Innovations for Defence Excellence (iDEX) and the formation of task forces of AI under the Ministry of Defence. This ensures dual responsibilities, including domestic invention while providing accountability and the international compliance on Humanitarian Law[8]. The Atmanirbhar Bharat has also been responsible for modernization of military over non-regulation of technological acceleration.

However, the nation needs to acquire legal preparedness remaining in the evolutionary process. The concepts of autonomous defence systems, military innovations, privacy accountability and international principles must reconcile in a fast-pacing converging domains for India's architecture that oversights sustainable assurance[9]. In conclusion, India's present legal position and policy framework provides for cautions but should be in a forward-looking stance and India must institutionalize cyber jurisprudence for harmonization for credible legislative norms and initiatives[10].

LITERATURE REVIEW:

In *Legal Regulation on artificial Intelligence in India a Human Rights Perspective by Sibi J Koola*, Artificial Intelligence (AI) enables machines to perform human like cognitive tasks such as learning, reasoning, and decision-making. However, there are significant human rights issues with its broad use, especially with relation to accountability, discrimination, and privacy. Although the body of law regarding AI's effects on basic rights is still developing, the Indian Constitution requires the State to stop such abuses. Moreover, Data protection, privacy, cybersecurity, and employment effect were listed as major issues in the 2018 Task Force Report, which also suggested frameworks for ethical deployment and regulation. It also emphasized the necessity of defining AI entities legally and striking a balance between individual rights and technical advancement. In general, India's developing AI governance uses organized, coordinated institutional procedures to handle ethical, legal, and human rights issues while fostering innovation. The main limitation of this paper is that it places too much focus on government initiatives without evaluating their execution or results. There is little study of current laws like the IT Act and the Digital Personal Data Protection Act, 2023, and the discussion of legal and ethical issues is shallow.

In *AI in the Indian Armed Services: An assessment, authored by Kartik Bommakanti*[11] the author analyses how doctrines of the Indian armed Services are not in complete alignment with existing operational practices and technological change. The doctrines of the Indian Armed Forces demonstrate a disjointed and antiquated conception of artificial intelligence (AI) in combat. Drones, semi-autonomous platforms, and surveillance systems are examples of technology that are presently in use, but their practical applications and strategic implications are not adequately captured by theories. The Air Force tackles AI under multiple names, the Navy hardly acknowledges it, and the Indian Army exaggerates its novelty. The

[6] https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

[7] https://www.idsa.in/publisher/issuebrief/india-and-the-global-laws-debates

[8] https://www.criminallawjournal.org/article/110/5-1-3-412.pdf

[9] https://www.ijfmr.com/papers/2025/2/41779.pdf

[10] https://carnegieendowment.org/posts/2024/02/indias-normative-stance-on-lethal-autonomous-weapons-systems

[11] https://ojs.indrastra.com/index.php/clawsjournal/article/view/124/130

tri-service philosophy, which lacks coherence and alignment with actual capabilities, is another example of this discrepancy. In general, India's defence strategy is still technologically sophisticated but doctrinally unchanged, considering AI to be an ideal rather than a cohesive and dynamic military tool. This mismatch leads to a situation where technology is being used, but without a consistent or officially approved conceptual framework guiding its deployment, accountability, or ethical considerations. Although this paper insightfully highlights doctrinal gaps in India's military approach to AI, it lacks empirical evidence, comparative analysis, and practical recommendations.

In *India's Regulatory and Ethical Stance on Autonomous Weapon Systems by Anviksha Pachori and Abhishek Bhati* the article argues that Autonomous Weapon Systems (AWS) find it difficult to understand intricate urban combat situations, which could result in algorithmic unfairness, misidentification, and injury to civilians. The question of who should be held accountable for any unintentional harm caused by the machine, the commanding officer, or the developer, remains a significant problem. It is a significant technical and moral problem to ensure that AWS can differentiate between military and civilian targets. India's dual objectives of responsible innovation and security readiness are reflected in its approach to AWS. India has not yet published a public doctrine defining "meaningful human control," despite the country's active development of AI-driven systems like armed drones and unmanned ground vehicles. Nonetheless, India's latest domestic AWS prototype incorporates human override procedures, stringent engagement guidelines, and ethical protections, demonstrating its dedication to supervision and accountability. In order to address the legal, technological, and governance issues surrounding military AI, the government has also hosted expert seminars and policy discussions. India supports for international rules to prevent misuse and promotes stopping the spread of AWS to non-state entities. In general, India aims to be a "responsible innovator" that harmonises its AI-driven defense strategy with accountability, transparency, and humanitarian ideals in order to strike a balance between technological advancement and ethical responsibility. This paper fails to address the gap between India's technological advancements and doctrinal or legal preparedness for AI-driven warfare.

In *Legal and Policy Implications of Autonomous Weapon Systems by Anoushka Soni & Elizabeth Dominic (Centre for Internet and Society, India), th*e authors emphasize that the absence of a universally accepted definition of Autonomous Weapon Systems (AWS) creates significant challenges in regulation and weapon review processes. It also points out that India presently lacks a well-defined public policy for AWS, has no proper review procedures, and encounters institutional challenges in guaranteeing accountability for its implementation. The paper also emphasizes dual-use technologies, export controls, and the expanding role of private defense businesses, emphasizing that regulation must take into account both commercial and governmental involvement. The authors advise adopting precise definitions, creating weapon review processes analogous to Article 36, guaranteeing accountability systems, and actively taking part in international norm-making in order to improve governance. However, this paper does not deeply analyse India's internal legislative process or procurement practices in great detail, and the reports are from 2020; given the rapid evolution of AI and AWS, more recent developments may not be covered.

In *Artificial Intelligence in the Cyber Battlefield: Legal Challenges in Liability, Attribution, and Forensic Evidence by Praveen Arya,* the study examines India's legal readiness to combat AI-driven cyberwarfare, focusing on three main issues: forensic evidence, attribution, and liability. The paper examines how AI-enabled autonomous and self-learning attacks expose the shortcomings of India's current legal system by challenging conventional legal ideas like purpose, causality, and foreseeability. Because the Indian Evidence Act of 1872 and the Information Technology Act of 2000 were not intended for autonomous systems, it is unclear who is responsible when AI acts on its own.

Furthermore, India's framework is still doctrinally weak and institutionally disorganised. It calls for reforms, such as changes to the IT Act specifically pertaining to AI, the creation of AI-Cyber Cells for forensic monitoring, and the adoption of a risk-based AI classification framework akin to the EU model to improve accountability, cybersecurity, and governance.

The major limitation of this paper is that it effectively highlights gaps in the IT Act and Evidence Act, it does not explore potential judicial interpretations or enforcement mechanisms.

LEGAL PREPAREDNESS:

"Owing to the numerous benefits brought about by technological advancements, cyberspace today is a common pool used by citizens, businesses, critical information infrastructure, the military and governments in a manner that makes it difficult to draw clear boundaries among these different groups”[12]. India has progressively integrated emerging technologies, particularly artificial intelligence (AI), autonomous weapon systems (AWS), and robotics into its military modernisation agenda. “Given India’s security needs and cross-border infiltration, a substantial number of investments in these areas reflects a strategic shift, enhancing operational effectiveness while minimising human risk during combat”[13]. “AI is bridging the gap by automating the detection and mitigation of Cyber threats, allowing faster response times and more accurate prediction of potential vulnerabilities” [14].

“After recognising technological modernisation as a priority as part of the national defence documents in 2017, the Indian Department of Defence Production (DDP) set up a multi- stakeholder task force with N. Chandrasekaran as the head to study the strategic implications of AI to provide military superiority. The MoD set up a high-level Defence Artificial Intelligence Council (DAIC) under the stewardship of Defence Minister Rajnath Singh and Defence AI Project Agency under the Chairmanship of Secretary DDP in 2019 to provide guidance to develop an operating framework and drive policy-level changes for AI adoption in the Indian military; the council was allocated an annual budget of INR 1,000 crore. With ambitions of becoming a global hub for AI, India is leveraging its uniquely evolved IT ecosystem and Defence Public Sector Undertakings to develop and design AI systems to support core defence operations”[15].

The Ministry of Electronics and Information Technology has established four committees to help encourage research in AI. An appropriate step in the direction of having a structured framework was taken by the Ministry of Industry and commerce when they set up an 18- member task force in 2017 to highlight and address the concerns and challenges in the adoption of artificial intelligence and facilitate the growth of such technology in India[16]. In accordance with the task force's proposal, the DDP established the Defence Artificial Intelligence Council (DAIC) under Raksha Mantri's chairmanship in order to offer the required structural support and guidance. The Department of Defence Production hosted the nation's inaugural Artificial Intelligence in Defence exhibition in New Delhi in July 2022. Defence Public Sector Undertakings, the Defence Research and Development Organisation (DRDO), and private enterprises have developed more than 75 AI-enabled defence products and technology. The Defence Artificial Intelligence Council (DAIC) oversaw the AI Def 2022. Even when many steps were taken to develop weapons and AI-driven equipment, India fails to enact laws that would regulate the complexities arising due to such development.

“On the one hand, AWS promises to enhance military capabilities, reduce the risk to soldiers, and potentially increase precision in targeting. On the other hand, their deployment in urban settings raises serious ethical and legal questions. Chief among these concerns is compliance with the core principles of IHL and human rights standards, particularly the principles of distinction and proportionality”[17]. “International legal debates on AWS have been ongoing in various forums, most prominently under the framework of the Convention on Certain Conventional Weapons (CCW) and its related Group of Governmental Experts (GGE) on Lethal Autonomous Weapons Systems (LAWS)”[18]. India is utilizing AI's potential to carry out tasks like gathering and analyzing data to monitor threats, detecting personnel and objects, anticipating logistical requirements, creating cost-effective approaches to missions, planning the future course of action, and stimulating human intelligence in addition to developing and acquiring offensive AI capabilities, such as Lethal Autonomous Weapon Systems.

India’s service-specific doctrines do not capture these distinctions and do not fully address the importance of AI and nor does the tri-service doctrine or Joint Doctrine of the Indian Armed Services of the Indian military address how AI might be relevant to military operations and missions[19]. The Indian Armed Force’s Service doctrine exhibit a disjointed and uneven comprehension of artificial intelligence (AI) and its military significance. AI is described as a "revolutionary"

[12] https://www.meity.gov.in/static/uploads/2024/02/National_cyber_security_policy-2013_0.pdf?utm_source=chatgpt.com

[13] https://apjihl.org/wp-content/uploads/2025/09/FINAL-Indias-Regulatory-and-Ethical-Stance-on-Autonomous-Weapons-Systems.pdf

[14] https://www.granthaalayahpublication.org/Arts-Journal/ShodhKosh/article/view/4144/3724

15

[16] Legal Regulation on Artificial Intelligence in India: A Human Rights Perspective, by Sibi Koola

technology that will likely influence future fighting in the Indian Army's Land Fighting Doctrine (IALWD), yet this perspective is logically incorrect. AI is already incorporated into current systems, such as UAVs and semi-autonomous platforms, and is not revolutionary but rather evolutionary. The ideology overstates the novelty of AI while neglecting to describe its practical integration or contemporary uses. The Indian Air Force (IAF), on the other hand, takes a more practical approach, recognizing the advantages and disadvantages of autonomous systems but rejecting the name "AI" in favor of Remotely Piloted Aircraft (RPAs), which are mostly utilized for Intelligence, Surveillance, and Reconnaissance (ISR) missions. The Indian Navy's doctrine barely addresses emerging technologies or AI at all, revealing an even deeper conceptual gap. These shortcomings are mirrored in the tri-service doctrine, which lacks consistency and does not match doctrinal claims with practical capabilities. When taken as a whole, the doctrines show conceptual ambiguity, institutional inertia, and a lack of strategic vision for the use of AI in combat. India's defense readiness is technologically ambitious but doctrinally deficient since they consider AI as an aspirational ideal rather than an organized and developing capability. In simpler terms, this means that although technology is advancing rapidly—through the introduction of AI, drones, surveillance systems, and automated logistics—the doctrines (official guiding manuals that govern strategy and operations) have not been updated to reflect these changes. One major lacuna in Indian law is the lack of any specific legislation acknowledging AI as a source of autonomous damage. It is not covered by either the Bhartiya Nyaya Sanhita or the IT Act. In situations where self-directed systems inflict injury, the omission deprives the courts and law enforcement of a legal foundation for establishing liability, bringing charges, or offering remedies.

COMPARATIVE ANALYSIS:

There is a plethora of definitions given by different countries for what is called as Autonomous Weapons. One such being, UK has provided a definition which centres in “intent and direction” that is focused on a higher level. The House of Lord’s Select Committee on Artificial Intelligence in UK does not have the primary focus on the intention of the system whereas its Inter-national partners focus on human non-intervention with those systems. This is considered to be a high threshold for autonomous that is capable of intention and direction. France has provided a definition in the same proportion where it explicitly defines that Autonomous Weapon Systems currently do not exist.

The governance of AWS has two significant detrimental scenarios, one is focusing of AWS where unfeasible technology diverts the focus from the pressing legal problems and its future as foreseeable. Second being, no understanding and intent present leading it to hypothetical AWS so it undermines a ban on it.

UNITED STATES:

In spite of all the convergence, US has developed both autonomous weapons and international discussions of LAWS that holds implications for congressional oversight, defence insights, military concepts of operations, treat-making policy and the was future. US is the most advanced and legally prepared nation for adopting AI-enabled Defense systems for cyber operations along with embedding legal and ethical oversights, that includes, Defense Innovation Board (DIB) AI Principles, 2019 and Department of Defense Chief Digital and AI Office (CDAO, 2022).

There is no prima facie agreed definition given out for an Autonomous Weapon Systems but Department of Defence Directive (DODD) has defined for the purpose of Military that are grounded for the target selection and decisions making engagement rather than the technological sophistication by the human operators. The role of human operator was designed to allow the operators and commanders to exercise appropriate levels of force that does not require any human control per se but rather broader involvement in decisions.

The US has also participated in the international communication discussions with LAWS, where they colloquially defined it as “killer robots” under the UN Convention on Certain Conventional Weapons (UN CCW) that happened in 2014, In 2017, this got transmitted from meeting of experts to a “Group of Governmental Experts” (GGE) and in 2018-

[17] R. Shahrullah and M. Saputra, above note 3, p. 2.
[18] R. Shahrullah and M. Saputra, above note 3, p. 2.
[19] https://ojs.indrastra.com/index.php/clawsjournal/article/view/124/130

2019, the GGE has taken the proposals by the state parties to affirm the political declarations about LAW, and to regulate the same. Even if the UN CCE is a consensus-based forum, the outcome that comes from it holds the implications on lethal autonomous weapons (LAWS)[20]. Nevertheless, US did not become a signatory to the binding treaty with LAWS, instead they adopted human accountability, technical reliability and Incremental norm development through multilateral forum.

Not only in warfare, but these principles extend to AI-driven cyber operations and espionage where the US has codified laws for legal structure of authority under its own nation or the domestic laws. Firstly, Cyber Command and Titles 10 which governs military operations under Dod, Title 50 of US Code which governs the intelligence and covert operations under Central Intelligence Agency (CIA) and National Security Agency (NSA). Secondly, Foreign Intelligence Surveillance Act Amendments Act of 2008 provided for surveillance and collection of date that requires warrants and judicial oversights for targeting US persons. Lastly, Computer Fraud and Abuse Amendment Act of 1986 that applies to malicious Ai-based hacking and cyber intrusions. Thus, AI tools used for espionage should comply with the dual legal regime, ensuring congressional oversights that was suggested by the Senate Select Committee on Intelligence.

In 2020, the SolarWinds breached a sophisticated supply chain attack where the Hackers belief was linked with the Russian state-sponsored group that inserted a backdoor named SUNBURST into the SolarWinds Orion software. The customers installed the software leading to malware. This attack was publicly disclosed which compromised many organizations that included U.S. Government companies. In conclusion, the U.S. set up governments to mandate standards for offensive Cyber Attack and this case was one of such key elements provided as an example for cyber warfare and espionage attacks[21].

UNITED NATION AND FRANCE SUBMISSIONS:

France and the UK have a close tie with a long history, that defines their mutual relationships in improving cooperation on defense and various international issues, including immigration and trade. A discussion initiated by France was launched with the UN's 1980 Convention on Certain Conventional Weapons (CCW) that acted as a response to the potential development of LAWS. The Alliance for Multilateralism event on September 26, 2019, saw the opening for endorsement of a declaration on LAWS prepared by France and Germany. This declaration is an example of the CCW's ongoing work, which uses the French Ministry for Europe and Foreign Affairs that sets out the 11 guiding principles to provide a framework for the development and use of autonomous weapons systems. India has eventually become one of the operators of this convention even before a signatory to it. This follows two distinct principles namely LAWS (Lethal Autonomous Weapon Systems) and PALWS (Partially Autonomous Lethal Weapon Systems) that deals in robotic meaning of decision making where PALWS cannot accurately define lethal decisions which modifies the field of operations. The major distinction between LAWS and PALWS is that the latter involves human involvement in certain situations.

Compared to India's domestic laws on cyberspace, intelligence, and weapons, France's Universal Jurisdictional reforms and national military law manual offer a more robust domestic legal framework. The UNGA and the President of the International Committee of the Red Cross has formed a resolution amended for a specific item that was given a title "Lethal Autonomous Weapon Systems". This autonomous weapon further states that it is targeting the humans by machines that has become a moral line that human beings must not cross. Argentina, Austria, Brazil and Bulgaria are supporting the negotiation of this legally binding instrument while Australia does not support it, along with Bosnia Herzegovina and Canada. Further, the Chair's summary on the Humanity at the Crossroads conference has worked with urgency including all the stakeholders for an international legal instrument for regulating the AWS[22].

[20] https://www.esd.whs.mil/portals/54/documents/d/issuances/dodd/300009p.pdf?utm_source=chatgpt.com

[21] https://rmcglobal.com/wp-content/uploads/2022/08/2020-SolarWinds-Hack-A-Case-Study-of-the-Russian- Cyber-Threat-July-2021

[22] https://www.stopkillerrobots.org/wp-content/uploads/2024/08/Overview-of-Submissions-UNSG-report-on-autonomous-weapons-FINAL

In the famous case of Nicaragua v. United States of America, the International Court of Justice found that the U.S. violated the law by providing support to the Parliamentary groups against the Nicaragua Government. The court ruled that it had no jurisdiction under the customary international law and in conclusion, it held that the actions by the U.S. Government were not justified as a group or collective self defense[23]. Another case being, Lafarge SA v. France, a legal proceeding against the French cement company and its payment to terrorist groups that included the Islamic State of Iraq and the Levant (ISIS) and al-Nusra Front, in 2013-2014 while operating in Syria. This became a case of criminal charges in both France and US with US authorities imposing complicity in crimes against humanity. The case is thought to establish a precedent for French courts to have jurisdiction over international crimes that French multinational firms commit elsewhere[24].

Therefore, under Article 36 of the International Humanitarian Law specifically provides for the Additional Protocol I (API) to the Geneva Conventions of 1949 that ensures new weapons are employed and developed in confirmation to the international laws.

ISRAEL:

Israel was always unique in providing its willingness to widely discuss it openly in the use of AI-based tools on the battlefield. The Israel Defence Forces (IDF) acknowledged the growing use of AI-based tool as part of the Israel's military arsenal where the trend became evident during the Israel-Gaza war in 2023-2024 where IDF deploys AI-systems as defensive mechanism, command and control, collection, processing and management of data for the offensive purposes. The State of Israel is a tech-savvy actor for the need of technological supremacy that drives Israel from the threats and cyber-attacks, especially during Israel-Hamas war. Some of the AI applications deployed by IDF include Proactive Forecasting, Threat Alert, targeting and Intelligence Analysis. This has also increased the role of international law in this aspect. In fact, the IDF explained that in order to guarantee significant human involvement in targeting decision-making processes, the choice of a target for attack by the Gospel will go through an additional independent review and approval by a number of other authorities (operational, legal, and intelligence).

It is crucial to remember that General Comment 36 of the Human Rights Committee adopted the stance that guaranteeing the protection of the right to life invites prophylactic impact assessment measures, including a legality review for new weapons and means of warfare, even though Israel is not a party to AP I and the customary status of Article 36 is being discussed. It included various aspects, three majorly being, no customary prohibition, legality of threatening or using nuclear weapons and human decision maker. Therefore, Israel has adopted new room for prudence while deploying military capabilities It not only foresees battlefield but also for the maintenance of international peace and security[25].

The psychological component of customary international law is called opinio juris, which refers to a state's conviction that a certain conduct is required by law rather than merely being convenient or habitual. It is one of two elements needed to create a norm of customary international law and the consistent state conduct is the other. In the absence of opinio juris, a state's actions would not be regarded as legally binding.

The Israel-Palestian war happened where media reports alleged the Israeli military for using Microsoft's cloud and AI surveillance which raised huge concern about the potential human rights abuses. In 2025, a review found that there were no evidences as to the date that Microsoft Azure and AI technologies have targeted or harmed people in Gaza. Thus, there is no time to delay and decision was taken with respect to Microsoft should take decisive action for ensuring they do not profit out of human right abuses of Palestian people by using AI technologies as Cyber Attack[26].

SOUTH KOREA:

The states that are continuously developing autonomous weapons are Russia, Israel, South Korea, China and United States. South Korea is generally classified as a technologically advanced country in terms of the development of Artificial Intelligence. There is something called the Korea Research Institute of Defense Technology Planning and Advancement (KRIT) which launched a map to leverage AI to future warfare. This identifies almost 272 AI-based core

[23] https://www.icj-cij.org/case

[24] https://conflictoflaws.net/2024/french-supreme-court-ruling-in-the-lafarge-case-the-private-international-law- side-of-transnational-criminal-litigations

technologies to advance military systems in surveillance, command and cyber security. The navigation towards warfare will be utilized for planning the development of defence equipment and discovering emerging military systems in the sector of national defence[27].

An arms race, or more accurately, a race to incorporate an increasing number of AI components into military systems, is frequently used to describe the application of AI in defense and security. After several attempts, South Korea has finally formulated its national strategy towards AI development within its defence policy in 2019. In order to plan for the use of AI across C4I, intelligence, firepower, maneuver, protection, and operational sustainment, the South Korean army established the AI Research and Development Centre within the Training and Doctrine Command that same year. The army plays a significant role in meeting AI priorities in defense. The South Korean Government has also been a major support towards the achievement of defence research and development with the help of many institutions including Defence Development and the Defense Agency for Technology and Quality, that falls under the Defense Acquisition Program Administration. In addition to these, the South Korean Aerospace Industries have developed a new unmanned aircraft as piloted fighter jet that operate froma safe distance.

The initiative taken by South Korea for combat aircraft as a step for development of unmanned aircraft in the future provides a solution for exploring autonomous flight capabilities by 2026. This initiative has been expected to progress to something called “semi-autonomous” formation flying combat. This aligns with the significant interest of Unmanned Combat Aerial Vehicles (UCAVs) displayed at the Seoul as complements to manned fighter[28].

The Institute for Digital Rights (IDR) has chronicled a number of significant issues in South Korea that highlight the nation's changing approach to AI regulation, especially with regard to accountability and privacy. The Personal Information Protection Commission (PIPC) launched investigations after AI-driven facial recognition systems installed in Seoul schools during the pandemic were accused of violating the Personal Information Protection Act (PIPA) by collecting students' biometric data without explicit consent. IDR and the National Human Rights Commission of Korea also criticized the National Police's implementation of an AI- based "Crime Prediction System" for possible algorithmic bias and inadequate legal control. Courts have started looking into algorithmic hiring and credit-scoring procedures in the private sector, highlighting the PIPA's requirement of openness and justice. When taken as a whole, these examples demonstrate South Korea's increasing awareness of the legal ramifications of AI, but they also illustrate the lack of a thorough legislative framework controlling the use of AI by the government or military[29].

Thus, the above demonstrated introductions made by South Korea has proved that the efforts towards AI-defense will significantly boost the capabilities relating to the regional adversaries by attracting potential customers worldwide[30].

<u>SUGGESTIONS AND WAY FORWARD</u>:

In order to guarantee accountability, adherence to international humanitarian law (IHL), and protection of national security interests, India's swift integration of artificial intelligence (AI), autonomous weapon systems (AWS), and cyber capabilities into its defence architecture calls for an equally strong institutional and legal framework. India's capacity to handle the moral and legal issues of AI-driven warfare has been undermined by the lack of a cohesive regulatory framework, gaps in attribution and liability procedures, and disjointed institutional coordination, despite significant advancements in defence modernization and technological innovation. Thus, following recommendations are given for

[25] https://opiniojuris.org/2024/04/20/artificial-intelligence-in-the-battlefield-a-perspective-from-israel

[26] https://www.hrw.org/news/2025/10/10/israel/palestine-microsoft-should-avoid-contributing-to-rights-abuses

[27] https://www.janes.com/osint-insights/defence-news/c4isr/south-korea-outlines-ai-plans-for-defence

[28] https://defencesecurityasia.com/en/south-koreas-kai-to-test-artificial-intelligence-ai-pilot-in-fa-50-light-combat-aircraft

[29] https://idr.jinbo.net/1917

[30] https://www.defensemagazine.com/article/south-korea-is-successfully-moving-forward-with-the-implementation-of-ai-in-the-defense-sector

improving India's operational capability, governance, and legal readiness in this developing domain:

1. India should critically examine the doctrinal insufficiency of the foundational frameworks regarding the complexities of liability, attributions and forensic evidences that arises from the autonomous AI systems leading to warfare. There seems a loophole in the recognition of statutory provisions for the acts that are committed by these AI- driven systems that leads the courts without a bias for either side of the parties. This can be helped by providing comprehensive legislation under the Information Technology Act, 2000 to clearly address the use of AI- system in defense, its accountability and liability mandating operational standards and risk-based clarifications.
2. The Indian armed forces must embed the principles of distinction, proportionality, and meaningful human control within training modules for all AI-based operations. This would ensure that automation in warfare does not compromise humanitarian obligations or civilian protection. The main focus lies on assessing the inter-agency coordination and collaboration that is required to tackle the cross-border digital threats and provide a resolution mechanism for the cybersecurity response team that lacks in the existing framework leading to disjointed cyber governance. Through a unified policy, India can ensure a credible offensive strategy.
3. India has always made a huge participation and alignment with international instruments and conventions. This should also be implemented for the defense mechanisms as it ensures a forward-looking frame that helps in human oversight and ethical cyber governance for application based on AI-systems. A regular parliamentary review be established to oversee the initiatives of cyber defense that provides humanitarian obligations along with the training modules for all operations relating to the preventive measures for AI-driven warfare.
4. A two-step verification system can be adopted, with the Cyber Department reviewing AI algorithms and training, followed by the Defence Department’s final assessment to ensure accountability and attribution.

CONCLUSION:

In conclusion, India is at a critical point where the incorporation of cyber capabilities, autonomous weapon systems (AWS), and artificial intelligence (AI) into its defense and security apparatus requires a corresponding transformation in its institutional and legal frameworks. With programs like iDEX, Defence Acquisition Procedure (DAP) 2020, and the bolstering of cyber organizations like CERT-In and NCIIPC, India has made significant strides in defense modernization; however, a crucial gap remains in the absence of a single legal framework governing AI-driven warfare and digital espionage. The critical need for comprehensive legislation that balances national security imperatives with the norms of International Humanitarian Law (IHL) is highlighted by the growing complexity of algorithmic decision-making, difficulties with attribution, and accountability in autonomous operations.

Therefore, all AI-based defense applications must incorporate human oversight, operational transparency, and ethical governance into a future-ready framework. Legal clarity and institutional accountability can be improved by establishing specialized judicial mechanisms, AI-forensic units, and parliamentary monitoring. Additionally, incorporating humanitarian concepts like proportionality and distinction into military training guarantees that moral and legal commitments are not compromised by technological dominance. India can improve its operational resilience and normative validity in the field of global digital security by coordinating domestic policies with international norms and strengthening interoperability between defense and cyber agencies. In the end, India's ability to develop a legally sound, morally sound, and institutionally cohesive defense governance will determine its readiness for AI-enabled conflict and espionage, not just technological advancement but also the framework for digital era.