ARTIFICIAL INTELLIGENCE-ENABLED CYBER WARFARE: A CRITICAL EXAMINATION OF NATIONAL SECURITY RISKS AND THE ADEQUACY OF INTERNATIONAL AND DOMESTIC LEGAL FRAMEWORKS

Gaurav Kumar Yadav, PhD Research Scholar, School of Law, Mahindra University

Madabushi Venkata Vasudev, PhD Research Scholar, School of Law, Mahindra University

Dr. Rishi Raj Bhardwaj, Assistant Professor, School of Law, Mahindra University

ABSTRACT

Cyber warfare is the domain where autonomous, huge, and adaptive cyber operations driven by AI have transformed warfare by significantly minimizing human participation in decision-making. The application of AI to both offensive and defensive cyber domains has brought forth unprecedented levels of, difficulty and occurrence of, and speed of cyber operations leading to new forms of international security and global legal order. The use of AI in cyber warfare enables more potent cyberattacks via advanced functionalities like automated vulnerability discovery, smart malware, data analytics predicting attack pathways, and disinformation. On the other hand, attribution, accountability, and conformism with the principles of established international law will continue to pose challenges as the employment of cyber tools that leverage AI to such a great degree continues to multiply and grow. Use of AI driven cyber tools is already raising grave concerns about IHL (International Humanitarian Law), law on use of force and states' responsibilities within cyber space. For a truth that is AI is an autonomous entity that challenges our most fundamental legal notions, including human control distinction, need, military operations and accountability, thus making the current legal regimes have major holes. In fact, the question that we really should ask is whether the present national and international legal regimes are fit to govern autonomous cyber operations during peacetime and in armed conflict. In this study, we inspect a series of controversial issues originating from the interplay between national security, the legal governance and AI enabled cyber warfare. The expansion of cyberspace as a theater of war, cyber vulnerabilities on the infrastructure of national security and the ever-growing threats posed largely

by AI-enabled malware, deepfakes, automated hacking and manipulation of info will be looked at. A number of relevant international legal documents, policy regulations on cybersecurity and states behavior along with historically relevant events such as the well-known STUXNET event have been utilized here as an aid to determine the capability of national legal and regulation to be able to face the emerging cyber threat. Furthermore, the study argues for a practical legal and policy framework aimed at fostering good governance of AI, development international collaboration, inspiring public-private cooperation, establishing strong rules on human control and answerability and acknowledgement of AI-powered operations in cyberspace.

KEYWORDS: AI, Digital World, Cyber Operations, Military Operation, National Security.

INRODUCTION

Human kind finds itself in very special and uncomforting circumstances in the 21st century. New technologies have opened up a world of both large risk and amazing growth. Technology has always been the driving force behind the advancement growth of our culture, but this time the change has been so great that it has already started to transform the manner we make communications, the methods in which we learn govern ourselves as a society. From smartphones that bestows instant access to all human knowledge to machine learning system that can detect diseases more correctly than ever, technology to be opening the avenues for plethora of possibilities for improvising human life and all connected domains.[1] This progress has put AI in paradoxical but notable position. AI, on one hand, takes credits for numerous daily comforts, like smarts traffic control system, virtual assistants managing our lives, and through streaming of internet-based services. On the other hand, same tools and technologies are employed in the Defence sectors engaged in various military operations. This now has emerged as a material concern for every global or nation-specific citizens having substantial threat to global peace and security.[2] Artificial Intelligence has raised as a significant component in the security operations of today, bestows support with the offensive abilities such as AI hacking and malware creation along with its defensive tools such as pre-detections of threats as well as its counter-response through machine intelligences. The thin line of demarcation

[1] Braden R Allenby, *The Applied Ethics of Emerging Military and Security Technologies INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS* 52 (1st ed. 2015).
[2] Nitesh Kumar, *A Critical Analysis of Existing Legal Frameworks Governing Artificial Intelligence in Cyber Warfare* (2026).

between human and machine decision-making gets more and more indistinct with the exponential pace of AI, thereby raising difficult legal question about liability, ethics, and adherence with the international norms. Cybersecurity is not the only sector, where AI has been disruptive force; it is merely one of numerous sectors, where AI has come to be regarded as disruptive force. The modern Cyber-Defence system is heavily dependent on AI technologies to increase their capability to identify threats and strategize responses for actions, and possibly foresee various versions of vulnerabilities in the future.[3] The offensive side gains a whole new expansion of complexity with the AI. The system powered by AI cannot only designed highly personalized malware, but also exhibited autonomous attacks and even found weakness in the system at the speed of light. When AI system operates mostly without intervention of human, the circumstances become very intricated with regard to ethics and law. The risk of harm gets higher because AI is capable of doing cyberattacks in very short time, and it is quite a difficult task to pinpoint the attackers. Such technologies are accessible to both government and hackers who might use them for distinct reason such as war, sabotage, or spying.[4] The primary battlefield is now cyberspace, which transcends national borders and renders legacy security system inadequate. Cyber operations involving AI frequently defy conventional wisdom, as they can compromise networks, disrupt critical infrastructure, and alter data. National security is now threatened by ransomware attacks on hospitals, government hacking, and AI-driven disinformation campaigns.[5]

HISTORICAL CONTEXT OF CYBER-WARFARE

The period of modern warfare has witnessed a dramatic change in cyber-warfare and notable historical instances of hacking have been the key influence on the change of tactics and the close synchronization of digital warfare with the real-world ones has been exhibited more and more clearly. Major cyber operations have not only been done but they have also become the modern international relations and conflicts tool since 2007. The suspected Russian DDOS strikes on The first major example of state-sponsored cyber warfare was the cyberattack on Estonia in 2007 this was followed by Cyber-kinetic activities during Russia-Georgia war.[6]

[3] "*New Solutions for Cybersecurity*" (*MIT Press*, December 1, 2021) https://mitpress.mit.edu/9780262535373/new-solutions-for-cybersecurity/

[4] Fatima Anis & Mohammad Hammoudeh, *Weaponizing AI in Cyberattacks a Comparative Study of AI Powered Tools for Offensive Security*, ICFNDS (2024).

[5] Neil Davison, *A Legal Perspective: Autonomous Weapon Systems Under International Humanitarian Law*, United Nations Office of Disarmament Affairs (UNODA) Occasional Papers 5-18 (2018).

[6] Samuli Haataja, *The 2007 cyber-attacks against Estonia and international law on the use of force: an informational approach*, Taylor and Francis (Mar. 25, 2017),

Cyber tools can physically damage critical infrastructure, as exhibited by the 2010 Stuxnet attack.[7] Later, incidents such as Shamoon, Sony Pictures, the power grid in Ukraine, and Not Petya highlighted the growing threats to civilians and non-military targets.[8] Cyber operations increasingly targeting civilian infrastructure and political processes, as evidenced by the Not Petya attacks on the Ukrainian power grid and interference in US election.[9] Subsequent incident like as the SolarWinds Colonial pipeline and ongoing attacks on water and energy systems through 2025, exhibits the increasing complications and robustness of cyber warfare by government and non-government players.[10]

CURRENT CONFLICTS

Cyber-Warfare had already been established as powerful weapon by mid-2025 and crucial factors in the ongoing geopolitical rivalries, particularly in the one involving Russia and Ukraine and Israel and Iran. Cyber operations were the second front besides the physical military actions in the conflict between Israel and Iran, with the former accused of cutting off some of the latter's sources of funds, and stealing from latter's main cryptocurrency exchange. Iran response primarily used to gravity of the hacktivist methods that influence people's psyche, such as the media interruptions, the AI- driven phishing attacks and the false missile alerts focused at the Israeli techies. Although the numerous attempts were successfully thwarted, there have been reports of significant increase in Palestinian cyber intrusions on Israeli websites. To that end, the pro-Iran organisation have progressed beyond their original aim of securing the partnership of only the U.S. and the U.K. in the region, signalling a grander strategic design.[11] Along with this, Russia Cyber-Warfare against Ukraine remains large scale and complicated one. Thousands of cyber-attacks targeted Ukraine's critical infrastructure in 2024, and Russia used new malware and social engineering to target the government in 2025, while considering operations against European infrastructure. Ukraine-key cyber counter operations have affected Russian Defence companies, uranium mines, railroads, and telephone,

https://www.tandfonline.com/doi/abs/10.1080/17579961.2017.1377914.

[7] Christopher Whyte & Brian M Mazanec, *The future of cyber conflict Understanding Cyber Warfare* 6 (1st ed. 2018).

[8] Dominic Rushe, *Sony cyber-attack linked to North Korean government hackers, FBI says*, The Guardian (Dec. 19, 2014), https://www.theguardian.com/us-news/2014/dec/19/north-korea-responsible-sony-hack-us-official.

[9] "*Cyber-attacks during the Russian invasion of Ukraine*, Office for Budget Responsibility (Mar. 20, 2022), https://obr.uk/box/cyber-attacks-during-the-russian-invasion-of-ukraine/.

[10] Çalışkan E, *Cyber Conflict Game Theory: Strategic Analysis of Global Cyber Crises in the 2000s*, Security and Defence Quarterly, 52, (2025).

[11] M. Sexton, *AI and the Evolution of Asymmetric Cyber Warfare: Insights from the 2025 Israel-Iran Conflict*, AI and the Evolution of Asymmetric Cyber Warfare: https://trendsgroup.org/insight/ai-and-the-evolution-of-asymmetric-cyber-warfare-insights-from-the-2025-israel-iran-conflict/.

system. The risks of large scale and well-planned cyber assault on the infrastructure of the West and the allies are becoming more pronounced with the establishment of the cyber partnership between Russia and Iran that includes the sharing of tools and technologies.[12]

AI ENABLED CYBER WARFARE AND NATIONAL SECURITY THREATS

One of the most crucial developments in the history of warfare is Cyber-Warfare powered by artificial intelligence. The battles conducted via invisible digital channels are increasingly replacing the classical war scenes like the movements of troops, the use of tanks, and the aerial fights. In this domain, the computer system running on algorithms are capable quickly performing the process of collecting and checking the data of vast sizes to discover vulnerabilities, make the selection of targets, and even predicts the timing of attack all without human involvement. This perspective has been completely transformed by the advent of AI system, which use algorithm trained on complicated and often inaccurate datasets to make decisions in life-and-death situations. There are large concerns regarding governance, law, and morality, when such delegations occur.[13] The use of AI in military operations is enhanced, especially when it comes to making autonomous tactical decision greatly disputes the conventional views about military actions', morality, legality, and accountability. The European chivalric codes and the Hindu notion of Dharma-Yuddha are among the numerous cultural frameworks that have underscored the necessity for moral and legal limits. Finally, but most importantly, today's International Humanitarian Law can be upheld by drawing on these moral precepts. The Geneva Convention of 1949and the Additional Protocols of 1977 serves as the cornerstone of the present legal system governing conflicts.[14]

These treaties contribute to the establishment of core principles of differentiation, proportionality, and precaution by making the parties concerned identify civilians and combatants, inhibit unnecessary harm, and take measures to maintain the lives of the civilians. Additional Protocol I Articles 48,51, and 52 are the most important clauses governing military operations. The use of AI-enable military systems and autonomous weapons in ongoing conflicts such as those middle-east and Ukraine raises difficult questions about the applications

[12] Kris Jackson, *The Unseen War: Cyber Warfare in the Shadow of Global Conflicts*, (July 8, 2025), https://www.cobalt.io/blog/the-unseen-war-cyber-warfare-in-the-shadow-of-global-conflicts.
[13] Fabio Cristiano et al., *Artificial Intelligence and International Conflict in Cyberspace (Routledge)* (1st ed. 2023).
[14] Dr Vincent Boulanin, Dr Lora Saalman, et al., *"Artificial Intelligence, Strategic Stability and Nuclear Risk"* (*SIPRI*, June 2020) https://www.sipri.org/publications/2020/policy-reports/artificial-intelligence-strategic-stability-and-nuclear-risk

of these principles when, in the future, combat and targeting decisions are made by machines rather that humans.[15] The internal legal and institutional progress of India is indicative of the states key actions to change the governance structures as countermeasures to the quick technology growth. The governance in India during the first few decades after the country independence was largely reliant on the rules comes from colonial era and were designed for conventional ways of communications and physical places thus very little had been done to manage new cyber technology-related crimes often depended on outdated legal provisions which are not suitable for modern digital threats. Thus the I.T. Act was enacted in 2000 which laid down the basic rules for data protection, intermediary liabilities and e-commerce. The 2008 Mumbai attack, which expose the serios flaws in the Intelligence and cybersecurity system, led to major institutional reforms including the modification of I.T Act, the establishment National Cyber Coordination Centre and NAATGRID. Since the establishment of organizations such as Défense AI Council (DAIPA) and the Défense Cyber Agency in 2018, which exhibited a tactical shift towards AI-driven national security management India has gradually integrated AI into Défense.[16]

DEEPFAKE, DISINFORMATION COMPAIGNS & THREATS TO CRTICAL INFRASTRUCTURE AND NATIONAL DEFENCE

Deepfakes and Disinformation campaigns are Nowadays being used as a psychological operation in modern cyber and information warfare, which have foundationally changed the battleground and moved it to the digital and cognitive spheres. Deepfakes are the computer-generated synthetic material that mimics real people and life incidents and may include, voice, video, images. By leveraging one of the basic human characteristics the trust in what one sees and hears these practices enable malefactors to create extremely and even shocking realistic impressions of public figures opinions or behaviours. Such AI generated content spreads quickly on social media, often before fact-checking is possible and thus, it is already eroding public trust in the information sources. This creates a misconception about reality and truth, which harms not only people but democratic process and society also.[17]

The growing use of Deepfake is a sign of key change in the way of Cyber-Warfare is conducted.

[15] Ibid
[16] Swaraj Paul Barooah et al., *The AI Task Force Report -the First Steps Towards India's AI Framework*, SSRN Electronic (2018). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5337308
[17] Petrica Gabriel, "*Deepfakes, Disinformation & CYBER-WARFARE*" (*IJISC*, June 30, 2025) https://www.ijisc.com/year-2025-issue-1-article-0/

Deepfake operations leverages the human natural tendency to acknowledge audiovisual information as true, unlike the conventional hacks that penetrate system and networks. When combined with digital echo chambers and social media algorithms, deepfakes have the potential to drastically alter public opinions and contribute to the deepening of social rifts, and even wipe out the legitimacy of public institutions.[18] In times of war, the capability of deepfakes to mislead by creating fictional incidents involving the army and issuing false claims about military and political figures makes them powerful propaganda tools. The dissemination of this sort of altered content happened at very quick pace over digital channels, often to overtake government reaction and fact-checking mechanisms. Consequently, conflicts can escalate, misinformation can spread and the resulting instability may be real.[19] India also faced the similar problem, with AI-generated fake content being the cause of political debates and even controversial national security incidents.

A multimodal outlook is needed to tackle the problem of AI-based psychological warfare, which includes raising the awareness of the public, having adaptable laws, and using state-of-the-art technology for detection.[20] The Cyber-Warfare enhanced by AI bestows the adversaries with a capability to direct very intricated, fully automated attacks on crucial system which, in turn, lead to serious threats to the core infrastructure and national security. Critical infrastructure includes important power supplies, water supplies, sanitary facilities, transport system and communications lines all of which are controlled by industrial and digital systems are very complicated and interconnected, hence they are more vulnerable. Such weakness may be taken advantages of by automated intrusion tools and cause, and non-negligible failures, and compromise military readiness, economic robustness, and policy safeguard.[21] Government and security companies faces a strategic problem in safeguarding against asymmetric AI threats, as

[18] Aroon Deep, *IT Ministry proposes mandatory labelling of AI-generated content on social media*, The Hindu (Oct. 22, 2025), https://www.thehindu.com/news/national/it-ministry-proposes-strict-rules-for-labelling-deepfakes-amidaimisuse/article70189322.ece.
[19] Aishwarya Khosla, *Warfare at night, deepfakes by day: The anatomy of a rumour in modern era conflicts*, The Indian Express (May 27, 2025), https://indianexpress.com/article/india/pixels-propaganda-panic-anatomy-global-conflicts-modern-era-10031598/.
[20] Adrienne Thompson, *The Existential Threat of AI-Enhanced Disinformation Operations*, Center for Security and Emerging Technology (July 11, 2022), https://cset.georgetown.edu/article/the-existential-threat-of-ai-enhanced-disinformation-operations/.
[21] Iot Security Institute, "*AI-Driven Attack Vectors: Critical Infrastructure Protection Challenges for Governments and Enterprises" IoT Security Institute (IoTSI)* https://iotsecurityinstitute.com/iotsec/iot-security-institute-cyber-security-articles/238-ai-driven-attack-vectors-critical-infrastructure-protection-challenges-for-governments-and-enterprises?

an attacker only needs to succeed once to cause significant damage.[22]

INTERNATIONAL AND NATIONAL LEGAL IMPLICATIONS

THE CHALLENGES: TOWARDS DEFINING THE CYBERSPACE

The absence of clear legal definition of Cyber-Warfare is serious barriers to the gradual progress of law and governance policies at the international level. Unlike conventional warfare which is dealt with through strong legal framework such as the Geneva Convention, Cyber-Warfare remains largely unregulated. A key issue is the lack of clarity in cyber realm, where attacks can be very difficult, if not impossible, to identify or read in the light of the purpose of the party that was attacked. The countries have different notion about cyber incidents; one state can ponder a DDoS (Distributed Denial of Service) attack as criminal act while another may see it as an assault or an act of political protest. This disagreement allows state to use their own judgment to greater extent, which poses a tactical benefit and also delays the establishment of common set of legal norms. In addition, the quick and continuous evaluation of cyber technology is an extra hurdle to effective governance and it also reveals the necessity for clear-cut legislative regulations that will not only cope with emerging risks but also get hold of cybercriminals.[23]

INTERNATIONAL LAW AND STATE RESPONSIBILITY

There is no consensus concerning the appropriate application of current international legal framework, involving United Nations Charter, to AI directed computer networks. The principles of jurisdiction and non-interference may trap a state as responsibility if it either facilitates or implements AI-based cyber-attacks against another state. Nevertheless, the complications of AI-operated tools, coupled with the invisibility of computer networks operations, makes attacks of this sort still very difficult to trace back to specific source. The use of AI in executing automated cyberattacks is on the rise, and this progress brings to the forefront ethical and legal concerns of valuable importance. One of the issues at stake is that autonomous system could conduct attacks without any human interference, a scenario that

[22] Kolawole Samuel Adebayo, *The Answer To AI-Driven Attacks On Critical Infrastructure: Resiliency*, (Mar. 25, 2025), https://www.forbes.com/sites/kolawolesamueladebayo/2025/03/25/the-answer-to-ai-driven-attacks-on-critical-infrastructure-resiliency/.

[23] Rajender Pell Reddy, *Cyber Warfare: National Security Implications and Strategic Defence Mechanisms"*, 73 International Journal of Computer Trends and Technology 48 (2025).

could lead to international law infringement and unintended causalities.[24]

Numerous worldwide steps have taken place to deal with the unlawful ambiguity of Cyber-Warfare such as "Tallin Manual" NATO, Cooperative Cyber Defence Centre of Excellence (CCDCOE) initiative and "United Nations Initiatives." Through the Tallin Manual, it becomes clearer how international law which in force today connects with cyber transactions as an authoritative interpretive guide formed by the world's top international law specialists. The manual is not binding but still plays a valuable role in formation of normative norms for Cyber-Warfare. To push the state agreement on the proper conduct in cyberspace, the UN has been advocating for multilateral initiatives and especially via the group government experts on advances in Information and Communication Technology in relation to global community.[25] These programs attempt to encourage international cooperation and trust-building, but significant differences among major countries still hamper consensus. There is uncertainty regarding the applications of existing international law to autonomous and offensive AI-driven cyber-technologies, while the Tallin Manual 2.0 support state responsibility for AI-enabled cyber activities originating from their territories.[26]

NATIONAL LEGAL FRAMEWORK

The changeover of conventional warfare to Cyber-Warfare has made critical civilian infrastructure like hospitals, banking system, and even water supply and communication system of private nature, susceptible to attacks by enemies. This transformation raised considerable constitutional questions for India, especially about the government capability to manage the conflict between the security of the nation and right to privacy, freedom, and dignity.[27] The norms that were meant for conventional warfare are now being put to the test by the new advancement where war is fought in the digital realm that is important for civil population. Accountability, supervision, respect for human dignity is mandated under India's Constitutional law framework and laws particularly Information and Technology Act of 2000, in dealing with the situation. The Indian legal system not only adhere to International Humanitarian law but also ensure that rights, checks, responsibilities, and justice govern Cyber-

[24] Dr. Saket. Vyas, "*ARTIFICIAL INTELLIGENCE IN CYBER THREATS: A LEGAL AND ETHICAL EXAMINATION*" 5 Indian Journal of Integrated Research in Law 813, (2025)
[25] Joseph E Stiglitz, *Addressing Climate Change Through Price and Non-Price Interventions*, 119 European Economic Review 594-612 (2019).
[26] Michael N Schmitt, *Tallinn Manual 2.0 On the International Law Applicable To Cyber Operations (Cambridge University Press* 1st ed. 2020).
[27] Constitution of India, 1950, Art. 14, 19 & 21

Warfare along with its commitments to international humanitarian law standards.[28]

ARTICLE 21 & 19 CONSTITUTION OF INDIA

As per the Indian Constitution no one can be deprived of his life and also personal liberty except in accordance the procedure establish by law. Over time, courts interpreted this clause broadly to include numerous fundamental rights, the most crucial one is the right to privacy. the supreme court decision in Maneka Gandhi v. Union of India (1978), it establishes the requirement for the government to comply with fundamental rights which must be respected by all authorities in the country. which held that all procedures affecting not only the life but also liberty which must be just, fair and reasonable, successfully incorporated due process of law into Indian Constitution. This decision turned out to be a precursor to the recognition of data and digital privacy.[29] In 2017 case of Justice K.S. Puttaswamy v. Union of India, (2017)[30] Supreme Court declared that any government intervention must satisfy the need of law, necessity, and proportionality and held privacy as fundamental rights under article 21. Article 19(1)(a), which enshrines in Constitution of India bestows Freedom of speech as well as expression also which includes right to express oneself digitally, subject to reasonable restrictions under Article 19(2). The Supreme Court in case of Shreya Singhal v. Union of India (2015) forced the government to respect online speech and to stop from placing unreasonable restrictions to it.[31] To ensure constitutional governance in the field of technological advancement, Article 246 and 7th Schedule divide the power between union, state and concurrent list. This permit parliament to enact laws on Cybersecurity, artificial intelligence, and national security under the residuary powers and union list.[32] The notion of pith and substance along with the residual powers of parliament come into play and help to fill up the vacuum when artificial and cyber technologies advance at fast pace. In State of West Bengal v. Union of India, (1963), supreme court upheld the union's legislative jurisdiction over the subject of national interest, international facets, and national security, thereby illustrating how courts clarify this balancing act.[33]

[28] J.N Pandey and S. S Srivastava, "*Constitutional Law of India"* 213 (Central Law Agency 62nd edn, 2025)
[29] *Maneka Gandhi vs Union of India* (1978 AIR 597, 1978 SCR (2) 621)
[30] Justice KS Puttaswamy (Retd) v Union of India, (2017) 10 SCC 1, para 638)
[31] Shreya Singhal v. Union of India, ((2015) 5 SCC 1.)
[32] Constitution of India, 1950, Art. 14
[33] State of West Bengal v. Union of India, (1963) AIR 1241 SC

INFORMATION TECHNOLOGY ACT 2000.

The I.T. Act 2000 remain in effect to address cyber threats posed by Artificial Intelligence. It forms the foundation of India's legal framework for dealing with cyber threat. The IT Amendment Act 2008, come into force and widened the scope of act. Act makes hacking and unauthorized access to computers illegal under section 66 which bestows maximum imprisonment of 3 years or fine of 5 lakhs Rs. Identity theft is punishable by maximum term of 3 years imprisonment and fine under section 66C and Data Breaches under section 43A, which establishes legal liability for failing to safeguard sensitive personal data. Section 70 inhibit unauthorized access to critical infrastructure, such as electrical grid, military networks and prescribes the punishment for 10 years in prison for the offense.[34] Cyberterrorism a notion that encompasses computer resource-based activities that put danger the security of nation, falls under the scope of section 66F which impose life imprisonment as punishment.[35] Even though the act does not bestows particular regulations for AI, its broad-based provisions make it possible to take legal action against cyber-crimes committed with the help of AI. In Shreya Singhal v. Union of India (2015) the Supreme Court declared that cyber restriction to protect national security are permissible as long as constitutional balance is maintained, but it also struck down section 66A for restricting freedom of speech.[36]

CONCLUSION AND SUGGESTIONS

The conflict has undergone a considerable transformation due to the use of AI-assisted Cyber-Warfare to great degree, which makes the differences among civilians and military personnel, periods of war and peace, as well as ambiguous security and individual rights issues. The use of AI in cyber operations has not only enhanced prerogatives of attackers but also those of the defenders who are now capable to retaliate in ways that are fast, automated, and most cases unrecognizable by the outside world. Among the others things, the UN Charter and International Humanitarian Law were not designed for this kind of situation; rather they were drafted without pondering the possibility of automated combat and thus, they face challenges of different nature with respect with responsibility, imposition, proportionality, and human control. India's safeguard under Article 14,19, & 21 and statutory measures such as the I.T Act 2000 are mostly reactive and technology-neutral even though they bestow a key right-based

[34] Information Technology Act, 2000, section 66, 66C, 43A, 70
[35] Information Technology Act, 2000, section 66F
[36] Shreya Singhal v. Union of India, ((2015) 5 SCC 1.)

framework at national level. The court played important role in maintaining a balance between security and freedom, but the non-existence of AI-specific regulations has resulted in large regulatory gaps. Legal reforms will have to be quick otherwise AI cyber operation will be able to totally eradicate democratic responsibility, human rights, and even the law.

- A legally enforceable worldwide framework for A-enable Cyber-Warfare should be created based on the Tallin Manual and UN Group of Governmental Experts (GGE) guidelines.

- Revise of enact the specific cybersecurity and AI Law that addresses crucial infrastructure, accountability, and autonomy.

- The supervision of cyber activities must be via independent organizations and with the help of judges with knowledge of issue

- Stimulate the application of digital literacy methods for protection of information integrity and the detection of deepfake.

- Any cyber action should be carried out in pursuance with the Puttaswamy standard of proportionality and legality.