INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD
ISSN(O): 2455-0620 [Impact Factor: 9.47]
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value : 86.87
Volume - 10, Issue - 11, November - 2024

DOIs:10.2015/IJIRMF/202411016 --:-- Research Paper / Article / Review

Balancing Innovation and Security: Artificial Intelligence and Legal Approaches to Cyber Terrorism

Ashana Mishra
Research Scholar, Department of Law, University of Mumbai
Email - ashana.mishra@gmail.com

Abstract: *In comfort lies discomfort, this has been a thought that has travelled through generations and speaking of comfort, who does not want to subscribe to it. The present context lies in the humungous leap that technology has taken and the myriad aspects it has exposed, some explicit while some still surfacing in the figment of our imagination. The job here is of 'thinking' and the sweeping changes has somewhere deprived us of our mental faculties in the area of weaving our thoughts to generate output. A little thing to ponder upon since the only thing that sets humans apart is the ability and the art of thinking. Indeed, an art for it is from this art that the idea of a gigantic technology germinated and today breathes life. The threat however lies in the fact that this technology might rob us of this art. While this was all on a philosophical plane, talking about the real and on ground challenges we are facing and may face in the future is that there is evidence to show that a looming danger follows this comfort ridden technology. The arena of cyber terrorism has witnessed immeasurable threat since the territorial boundaries have dissipated and that of crimes via the means of technology has only multiplied. The hanging question revolves around the fact that how Artificial Intelligence can really further the momentum of crimes by technology or can it aid in controlling it. This paper is an attempt to assess both sides of this conundrum. The paper focusses on understanding the nitty-gritties of Artificial Intelligence and Cyber Terrorism and the nexus between the two. Also, how law plays a catalyst in containing the excesses of potential threat of AI and the threats of cyber terrorism.*

Key Words: *Artificial Intelligence, Cyber Crime, Cyber Terrorism, Law, Justice.*

"The development of full artificial intelligence could spell the end of the human race…. It would take off on its own, and re-design itself at an ever-increasing rate. Humans, who are limited by slow biological evolution, couldn't compete, and would be superseded."[1] -

Stephen Hawking, BBC

1. INTRODUCTION:

This paper, at the outset lays down a basic framework of understanding the basic notions underlying AI and Cyber terrorism. It then expands to the various facets that underline the endless possibilities that AI offers in the field of cyber security and the potential threats that the same system may pose. Understanding AI is no child's play, the term has undergone myriad interpretations and connotations ascribed to it by experts and various stakeholders. It thus becomes incumbent on us to cage the understanding of this giant technological development to assess the possibilities and handicaps so that remedial measures can be safely drawn after the thorough study.

2. Research objectives :

1. To understand the basics of Artificial Intelligence.
2. To provide a summative understanding of Cyber Terrorism.
3. To study the nexus between Artificial Intelligence and Cyber Terrorism.

[1] Cellan-Jones, R. (2014) *Stephen Hawking warns artificial intelligence could end mankind, BBC News*. Available at: https://www.bbc.com/news/technology-30290540 (Accessed: 27 January 2024).

4. To analyse comprehensively the laws in place in India and across borders that cater to combating challenges posed by Cyber Terrorism.
5. To study legal approaches of jurisdictions in the domain of cyber terrorism.

3. RESEARCH METHODOLOGY :

As has been defined by Albert Scent Gyorgyi[2] *"Research is to see what everybody else has seen and think what nobody has thought"*. This paper seeks to adopt the doctrinal approach of study. The researcher aims to study the pool of literature and the works of experts in this domain and present a novel aspect to this area of research. The central theme being to get into the anatomy of extensive literature and conduct a thorough study about the growth of AI and its close nexus in both containing the dangers of cyber terrorism and also its catalyst role in multiplying its dangers. This research has been done by thoroughly examining the existing principles, statutes and case laws relevant to the subject matter of study. It incorporates the use of both primary and secondary resources to enable the researcher to identify and interpret and develop a critique in the field of Artificial Intelligence and Cyber Terrorism.

The researcher, at the outset scrutinised the legislations in place to build a detailed understanding of the existing framework and challenges surrounding the same. Case studies were included to assess the real-world scenario in this field of study. The secondary sources such as scholarly articles, case commentaries and textbooks were also thoroughly engaged to build a more textual perspective in this domain of study.

The researcher while employing the doctrinal method of research has sought to delve into the principles and its practical implications while at the same drawing a critique and highlighting the limitations in the current landscape. This method has helped the researcher in ensuring that a structured and systematic exploration of the law and literature can be undertaken to provide more clarity in the present landscape of AI and Cyber Terrorism.

Legal Cloak in The Field of AI and Law and Cyber Terrorism

- **The Budapest Convention on Cybercrime[3] (Council of Europe)**

This is perhaps the first international treaty aimed at addressing internet, technology and cyber related crimes. It aims at harmonizing various national laws and fostering better investigative techniques by urging better cooperation amongst nations. The convention spans across aspects of cybercrimes and includes offences violating confidentiality, integrity, computer induced fraud, child pornography and also tangents of copyright infringement. It envisions the creation of a common criminal policy to protect the society from such unprecedented attacks by the ever-growing technological advancements.

It lays down certain substantive criminal law provisions ranging from illegal access, illegal interception, system and data interference and misuse of devices. Amongst the procedural safeguards it calls for expedited preservation of stored computer data, granting law enforcement agencies to search and seize stored data, collection of traffic data to aid criminal investigations and interception of content data under certain caveat.

The convention has gained momentum as more than 60 nations have ratified it and have framed protective policies on similar lines.

- **The Information Technology Act, 2000 (India)**

With the advent of the IT Act, 2000, the sensitivity around the issue of cyber laws and cybercrimes have only gained paramount momentum. The act has covered a vast plane of issues in this landscape which includes:

- Identity Theft
- Cyber Bullying
- Cyber Terrorism
- Hacking
- Trade secrets
- Defamation
- Harassment and Stalking

The act underwent amendments in 2008 in light of the growing concerns over cybercrimes. The act expands the idea of cybercrimes spanning across three domains namely, individual, property and government.

[2] https://www.nobelprize.org/prizes/medicine/1937/szent-gyorgyi/facts/ - accessed on 27.07.2024
[3] https://www.coe.int/en/web/cybercrime/the-budapest-convention - accessed on 15.08.2024

- **Computer Fraud and Abuse Act (CFAA) (United States)**

This is a Cyber Security law in the United States which outlaws the conduct that in any way victimises the computer systems. It lays down regulations for protection of federal computer systems, bank systems and other systems connected to the internet. It covers a wide arena of subject matter such as computer trespassing of government computer systems, damaging a government computer by way of hacking that leaves the sensitive data in a state of vulnerable exposure, committing fraud that is done by unauthorised access to a government computer, trafficking in passwords that affects interstate commerce, committing espionage by accessing the government computer. This act enables stringent provisions which not only defines the offences but also makes it a crime even attempt or conspire to commit such offences.

What is Artificial Intelligence?

Artificial Intelligence (hereinafter referred to as AI) has surfaced and resurfaced in the recent years owing to its transcendental growth. The users of AI have applauded the ease that has seeped into myriad arenas. While its potentiality is indeed laudable, yet the wave of concerns has still posed pertinent questions. How real is the artificial element and how intelligent is this intelligence ordained system? While these questions are being deliberated and will continue to form a part of deliberations for years to come, we can only focus on the advantages we have been bestowed with and the neighbouring challenges that these advantages have been accompanied with.

Let's first address the elephant in the room before we get to assessing its contributions and contradictions. The term AI has been put under the lens of myriad definition, but the pertinent issue is can this ever-growing giant be confined to a single definition? The experts have pooled in their natural intelligence to define this human created artificial intelligence. John McCarthy[4] had defined it as "the science and engineering of making intelligent machines".[5] This simply implies that any intelligent machine made with the intervention of human beings used by human beings to aid in work which humans do. So, who is the more intelligent being here? Humans or human engineered or created machines? Another definition of AI deems it as "a technical and scientific field devoted to the engineered system that generates outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives"[6] This definition too touches upon the element of human intervention in the creation of AI. A summative understanding of various definition ideates a meaning that AI is branch of intelligence that has been created for specified objectives with the help of algorithms.

Understanding Cyber Terrorism

Ever since the world has been under the influence of computers and technology, activities have remain barely confined by boundaries. Businesses have expanded, countries have developed ties and many more instances of positive developments. However, this advent has not remained untouched by the downside of it. Technology sees no boundaries and one such area which has had the worst impact is the domain of cyber terrorism.

Cyber terrorism in simple terms has been defined as "acts of terrorism transcending national boundaries"[7] . Defence analyst Dorothy Denning has defined cyber terrorism as *"Unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."*[8]

Nexus between AI and Cyber Terrorism

The multifaceted nature of AI speaks for its own ability to both aid in collection of data and organising the same. It has also become equipped to protect this data. This advent can be studied under two heads; Potential Advantages and Potential Threats.

4. POTENTIAL ADVANTAGES

AI can offer multiple ways of acting as a boon to deal with the cyber menace. A well trained and regulated AI system can aid in:

[4] https://computerhistory.org/profile/john-mccarthy/ - accessed on 27.07.2024
[5] https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf - accessed on 27.07.2024
[6] https://www.iso.org/artificial-intelligence/what-is-ai - accessed on 27.07.2024
[7] U.S. Patriot Act 18 U.S.C. 2332b
[8] https://online.fdu.edu/program-resources/cybersecurity-and-cyber-terrorism/ - accessed on 27.07.2024

- **Assessing Behaviour Patterns:**

AI has the potential of identifying anomalies and of determining abnormal behaviour in the algorithmic patterns. It can study the users, the activities conducted through systems, manage IP addresses, study the change in any files and folders and also in filtering out relevant data from irrelevant pool of data.

- **Outcome Predictability**:

Upon assessing any unusual pattern or behaviour, AI systems can be trained to rake up necessary solutions and to provide the future incremental steps that would address such behaviour and this can result in generating automated response to potential threats. This can be done by immediately blocking any malicious activity.[9]

- **Cost-Efficient approach:**

The traditional tasks performed by human analysts and IT Security Consultants can now be done in a more cost-efficient manner by the fusion based approach of incorporating both Artificial Intelligence and Machine Learning systems. This would imply saving not just the expenditure of organisations but also the number of hours. The idea is not replacement of human security administrator but to only aid such experts in reaching far beyond defined human capabilities.

- **Monitoring the Dark Web:**

The Dark Web[10] is a disguised network of various websites and services which is ideally not accessible by the traditional search engines. Dark web is often used by cybercriminals to trade in stolen data wherein they engage in transactions that may include dealing with credit card information, the log in credentials and other such sensitive data of individuals and organisations. AI platforms and AI backed software can be trained to study dark web and identify the palpable threats and raise alarm for appropriate actions to be taken in the event of any such activity detected which could hamper organisations and individuals.

While the heightened benefits of AI in this regard is beyond comprehension, many users have expressed that there is potential threat that AI systems are susceptible to.[11]This has only opened floodgates into the myriad challenges that users and organisation have not initially anticipated. These threats only reflect the tangible contours of Cyber Terrorism.

5. POTENTIAL THREATS

The threats can be disguised in the form of:

- **Rampant automated attacks:**

AI's ability to mimic humans and the thought processes through its algorithms, while being celebrated as a breakthrough is equally alarming. Cyber criminals can easily ransack into the data systems by training the AI models to manipulate data and to wage coordinated cyber-attacks without human cyber-criminal involvement.[12] Organisations today are exposed to vulnerabilities because of the fast-paced cyber-attacks wherein millions of neural networks are working in a

[9] https://forbytes.com/blog/ai-in-cybersecurity/#4-major-advantages-of-using-ai-in-cybersecurity-for-your-business – accessed on 15.08.2024

[10] https://www.verizon.com/business/resources/articles/darknet-the-shady-underbelly-of-the-iceberg/ - accessed on 15.08.2024 - The dark web is one of the three parts of the World Wide Web.

1. The surface web, or Clearnet, is the part of the World Wide Web that most people use every day through search engines. It is a substantial, but small, fraction of the web (5 to 10 percent). No passwords are needed to connect to the surface web; you just search and browse. It includes search results from Google, Bing, Facebook, LinkedIn, YouTube, etc.
2. The deep web is the web beyond the surface web—search engines cannot index it, and deep web sites need authentication to access. Most people use parts of the deep web every day for accessing things like web mail, pay-walled news articles, non-public social media profiles and posts, etc. Deep web content also includes things like medical records, government records, missing persons information, and organization's website areas that are for internal use only.
3. The dark web is a small subset (4-5 percent) of the deep web. It is only accessible through a special browser. The Onion Router browser is the most well-known dark web browser, and is best known for the anonymity it offers its users. However, the dark web also includes other overlay networks that can only be accessed with specific software/configurations. These include peer-to-peer networks and anonymity networks like I2P, Freenet, Retro share, GNU net, Syndie, One Swarm and Tribler.

[11]https://sdi.ai/blog/artificial-intelligence-and-cyber-crime/#:~:text=One%20of%20the%20ways%20that,or%20respond%20to%2C%20cyber%20attacks. – accessed on 15.08.2024

[12] ibid

trained manner to hack into the sensitive data of these organisations. The training of these AI systems barely takes times as manoeuvring through the algorithms can be done in little to no time and once these systems pick up on the established patterns, it becomes further difficult to trace the origins of attack and to pin liability.

- **Hacking:**

The compilation, assimilation of data and the retrieving of such data once access has been tracked down has become an easy venture for hackers. The modern technological systems of today like that of object and facial recognition not only capture the superficial attributes in the security systems but a large pool of data is also captured by these systems. Access to such pool of data becomes a child's play for a hacker, all that is needed is access to the footage. This is indeed alarming as such technologies have been imbibed to garner security levels of individuals but such a loophole and lack of regulation may render more harm than good.

- **Tweaking algorithms**

A pattern change is all that need is needed for a hacker to break down the receptive skills of an AI system. What an AI system perceives as relevant and irrelevant data has become easy to feed. This can directly damage the whole machine learning process which is the thrust on which an AI system works. Once played with, it can lead to detrimental damage of the entire information system of the organisation. The United States and North Korea debacle is a paradigm example of how ugly can these targeted attacks can be. The whole geopolitical map can be shaken up by this planned cyber warfare that can directly launch critical attacks on established infrastructure and financial institutions.[13] The Lazarus Group[14], also known as APT38, the North Korean Cyber Gang has been in news for having forged coordinated attacks on several financial institutions and business, which is primarily aimed at targeting governments. The group has so far targeted South Korea largely but its cyber warfare has also roped in jurisdictions such as that of the United States and the like. The notorious historical account of their attacks ranges from Operation Troy[15], Sony Breach- Sabotage[16], Bangladesh Bank Cyber Heist[17] amongst the many. These instances are only a cursory reminder of what an unchecked AI system can be susceptible to and the damage that it can inflict upon a nation altogether rendering it vulnerable to further attacks. What seems to an even more glaring issue is the traceability of these attacks. A regulation in place and stringent filtering mechanism can perhaps be a starting point. However, these only reflect that 'intelligence' in the artificial domain has caused more damage to nations than yield advantages.

- **Bypassing Physical Recognition[18]:**

AI has been credited to mimicking humans in terms of thinking, subject to the algorithmic networks. It has also become capable of replicating the physical attributes and characteristics of certain individuals. A glaring example

[13] https://sdi.ai/blog/safeguarding-against-cyberwarfare/ - accessed on 15.08.2024

[14] Lazarus Group, otherwise known as **APT38**, is an infamous hacker group believed to be based in the North Korea. It's known for its sophisticated and highly coordinated cyber-attacks targeting governments, financial institutions, and businesses.
Recognised under aliases such as Guardians of Peace, Hidden Cobra, and APT38, Lazurus has been a prominent threat in the cybersecurity landscape since as early as 2009. Although it is not clear who is really behind the group, the US and other governments have linked the group to the government of the DPRK, commonly referred to as North Korea.

[15] Operation Troy," a cyber espionage initiative that unfolded between 2009 and 2012. During this period, the group leveraged malicious tools like My doom and Dozer to orchestrate a sizable but relatively rudimentary distributed denial-of-service (DDoS) against a swath of US and South Korean websites.

[16] In November 2014, the cyber world was rocked by a Reddit post signalling a devastating breach at Sony Pictures, attributed to a group calling themselves the "Guardians of Peace." The fallout was nothing short of catastrophic: stolen data flooded the internet, exposing unreleased blockbuster films, internal correspondence, and sensitive employee information encompassing over 4,000 individuals.

[17] In January 2015, several Bangladesh Bank employees received a seemingly harmless email from an individual identifying as Rasel Ahlam, a job seeker. The email courteously requested the recipients to download Rasel's CV and cover letter from a provided website link. However, investigations by the FBI later revealed that Rasel Ahlam was a fabricated identity used by the Lazarus Group. Regrettably, at least one bank employee fell victim to the deception, unwittingly downloading the documents and inadvertently infecting their system with concealed viruses. The cyberattack on Bangladesh Bank resulted in the theft of approximately $81 million. Some of the stolen funds were traced to casinos in Macau, highlighting the international reach and complexity of the cyber heist orchestrated by the Lazarus Group.

[18] https://sdi.ai/blog/artificial-intelligence-and-cyber-crime/#:~:text=One%20of%20the%20ways%20that,or%20respond%20to%2C%20cyber%20attacks. – accessed on 15.08.2024

of this can be traced back to the year 2019, when a hacker used AI to clone the voice of a European Company Executive[19] which led to a major Artificial Intelligence Heist.

6. LIMITATIONS :

While the amplitude of advantages may have expanding contours, the threats tend to disturb the balancing scales. In the field of managing AI in similar lines with Cyber Security, there are tangible limitations which makes one ponder on the handicaps that this exponentially growing field of AI can be exposed to[20]. These limitations also reflect the potential risks that heavy reliance on AI mechanisms can lead to:

- **The Inevitable Bias**:

Bias is no longer a domain of the human nature alone. It has transcended into the algorithmic domain as well and more so, one that cannot be deciphered easily. The interesting dichotomy here is that the bias of an AI system is reflective only of the extent of bias that a human can feed into it, especially in the narrow AI phase where human intervention is still dominant. The biased feeding can eventually lead to biased outcomes and will only hamper decision making in the long run. However, there are great examples of platforms such as the IBM Watson[21] and Cylance[22] that engage in thorough Machine learning training to reduce the element of bias.

- **Flawed Interpretation:**

AI systems have often been said to be exposed to hallucinations[23] wherein it tends to generate output that is not based on the training fed into the system. These can lead to flawed interpretations and often even to misinterpretations. This tendency of AI system can result in false detection of threats or improper threat assessment. Such episodes of false positives can also result in blocking of legitimate sites and operations.

AI hallucinations can be synonymous to how humans sometimes see figures in clouds. This can stem from multiple factors such as;

- Overfitting[24]
- Algorithm Bias
- High Model Complexity

The consequences of AI hallucinations can often lead to unprecedented consequences. To understand this from an example, a healthcare AI model[25] can wrongfully read a benign skin lesion as an issue that is malignant. Generative AI in the field of healthcare has to further tread on a line of caution. Such Generative AI Hallucinations[26] within the healthcare can pave way for ethical concerns and also open the pandoras box of risks which may also sometimes be beyond human comprehension. It thus becomes pertinent to examine the use of AI in the area of healthcare before taking a plunge into incorporating Generative AI in its broader context.

[19] https://www.washingtonpost.com/technology/2019/09/04/an-artificial-intelligence-first-voice-mimicking-software-reportedly-used-major-theft/ - accessed on 15.08.2024 - Thieves used voice-mimicking software to imitate a company executive's speech and dupe his subordinate into sending hundreds of thousands of dollars to a secret account, the company's insurer said, in a remarkable case that some researchers are calling one of the world's first publicly reported artificial-intelligence heists.
The managing director of a British energy company, believing his boss was on the phone, followed orders one Friday afternoon in March to wire more than $240,000 to an account in Hungary, said representatives from the French insurance giant Euler Hermes, which declined to name the company.

[20] https://forbytes.com/blog/ai-in-cybersecurity/#4-major-advantages-of-using-ai-in-cybersecurity-for-your-business – accessed on 15.08.2024

[21] https://www.ibm.com/blog/watson-nlu-bias-ai-sentiment-analysis/ -accessed on 15.08.2024

[22] https://www.solutionspt.com/cylance -accessed on 15.08.2024

[23] https://www.ibm.com/topics/ai-hallucinations - accessed on 15.08.2024 - AI hallucination is a phenomenon wherein a large language model (LLM)—often a generative AI chatbot or computer vision tool—perceives patter
ns or objects that are non-existent or imperceptible to human observers, creating outputs that are nonsensical or altogether inaccurate.

[24] In machine learning, overfitting occurs when an algorithm fits too closely or even exactly to its training data, resulting in a model that can't make accurate predictions or conclusions from any data other than the training data.

[25] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10552880/ - accessed on 15.08.2024

[26] https://aimresearch.co/cdo-insights/hallucinations-in-gen-ai-a-healthcare-industry-perspective-with-prashant-natarajan - accessed on 15.08.2024 - "Hallucinations" in Gen AI refer to instances where AI-generated content lacks factual accuracy or context, potentially leading to misinformation. In the healthcare industry, where accuracy is crucial, understanding and addressing these challenges are paramount.

- **Heavy Reliance:**

While many organisations may gravitate towards low-cost IT services, businesses may tend to become heavily reliant on AI systems. This may also attract complacency and the whole process may be deprived of qualified human oversight. Eventually this can add to the accumulation of AI errors in cyber security systems. This leaves organisations at a higher risk of vulnerability and data exposure. Many branches of AI systems can be trusted only if there is a human oversight involved. For example, cognitive computing[27] is a facet of AI that still needs the intervention of humans to deliver efficient outcomes.

- **Skills Gap:**

There is still a dearth of skilled IT professionals and managers in the industry. Their skills enable a smooth deployment of AI systems for the efficient management of cyber security systems but because of the shortage of these expert minds, there is still a palpable gap in this field. This can eventually lead to poor management and inadequacy to render protection against potential cyber threats. Thus, to expect aid of AI in the domain of cyber security, it is incremental to have professionals who can train the systems that would be effective rather than amateur systems that may result in such systems being more defective.

7. Key Findings :

During the course of this research study, the researcher has analysed that there are fair regulatory guidelines for jurisdictions to take charge of the challenging leap that cyberterrorism poses. But an alarming revelation is that the area of cybercrimes has only posed severe threats with the advent of AI. The field of AI itself has not been confined to a filtered set of understanding and this itself is a big challenge for the stakeholders to identify and then lay a blueprint of addressing the same. There is a robust framework for addressing concerns in the digital realm but with AI integration, there are significant challenges to deal with. This is owing to AI's self-learning ability and to evolve autonomously that makes it even more challenging to predict and control the threats. It may thus be a difficult task in mapping out a potential and holistic framework that would sink in with the adaptive regulations.

Consequences scale and the way forward

The advantages naturally seem to outweigh the anticipated consequences yet it is of paramount importance to crystallise the solutions for the anticipated consequences. The spectrum of AI is only growing and will grow multi-fold in years to come so with the abovementioned challenges there is an urgent need to counter the menace of data biasness and a transparency in the algorithmic domain. The specificity in the arena of cyber terrorism is furthermore important as any failure, no matter how miniscule can put individuals and organisations under the radar of heavy losses and susceptibility to liability.

The idea is to propose a more lucid plan to avoid any such ills in the system that incorporates AI to deliver justice. Some measures that can be needled through may include addressing bias and irregularities through regular data audits and debiasing mechanism, incorporating human oversight and intervention at stages where even a minute suspicion arises in the predictability of AI decisions. The other aspect would be to map out accountability through standardized regulations devised by the think tanks and policy makers by keeping in perspective the experiences of nations. The harms of AI only multiply under the umbrella of ignorance so campaigns to raise awareness through designed educational programmes at various levels would instil responsible handling of AI systems. The stakeholders in the arena of AI and Cyber law systems can be trained by the right minds before an advancement is made for weaving of AI system into the cybersecurity domain. There should also be a provision by respective governments to invest in alternative technologies and research platforms that would be in continued touch with studying the pros and cons and providing workable solutions in the same light. In a nutshell, the fundamental idea is envisioning a future of speedy justice while being able to strike a reasonable balance between the scales of convenience and consequences. This conundrum can wither away only with a strategic system to deal with the volatile challenges that may ensue in the way of justice delivery system. The way forward lies in contextual roadmap towards contextual consequences as the system of AI will at many stages also reveal its Achilles heel, the aim therefore should be effective redressal. These safeguards

[27] https://www.sisense.com/glossary/cognitive-computing/ - accessed on 15.08.2024 - Cognitive computing refers to the use of reasoning, language processing, machine learning, and human capabilities that help regular computing better solve problems and analyse data. By learning patterns and behaviours and becoming more intelligent, a computer system can tackle complex decision-making processes.

will help us achieve a future where justice delivery through AI inbuilt systems will become the norm and quick disposal of cases, a much waited and realised reality.

REFERENCES :

1. AI and Law

- Surden, H. (2019). Artificial Intelligence and Law: An Overview. *Georgia State University Law Review*, *35*(4), 1305-1330. https://doi.org/10.2139/ssrn.3411869
- McCarthy, J. (2007). What is Artificial Intelligence? *Stanford University*. http://jmc.stanford.edu/articles/whatisai/whatisai.pdf
- Wischmeyer, T., & Rademacher, T. (Eds.). (2020). *Regulating Artificial Intelligence*. Springer. https://doi.org/10.1007/978-3-030-32361-5

2. AI and Cybersecurity/Cyberterrorism

- Taddeo, M., & Floridi, L. (2018). How AI Can Be a Force for Good. *Science*, *361*(6404), 751-752. https://doi.org/10.1126/science.aat5991
- Wilson, C., & Reilly, J. (2021). AI and the Future of Cybersecurity: Key Challenges and Opportunities. *Journal of Cybersecurity Research*, *1*(1), 15-27. https://doi.org/10.1080/24701031.2021.1896514
- Schmitt, M. N. (2017). "Virtual" Disenfranchisement: Cyber Operations and the Jus ad Bellum. *Journal of Conflict and Security Law, 22*(1), 93-116. https://doi.org/10.1093/jcsl/krw012

3. Cyberterrorism

- Weimann, G. (2015). Cyberterrorism: How Real Is the Threat? *United States Institute of Peace Special Report*. https://www.usip.org/sites/default/files/SR119.pdf
- Conway, M. (2007). Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet. *Information & Security: An International Journal*, *12*(1), 59-72. https://doi.org/10.11610/isij.1202
- Jarvis, L., Macdonald, S., & Nouri, L. (2014). The Cyberterrorism Threat: Findings from a Survey of Researchers. *Studies in Conflict & Terrorism*, *37*(1), 68-90. https://doi.org/10.1080/1057610X.2014.853603