INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

ROLE OF AI IN CYBER CRIME AND HAMPERING NATIONAL SECURITY

AUTHORED BY: AKANKSHA CHAUHAN
Qualification: B.A LLB (Hons), M.A Security and Defence Laws

Emergence of Cyber Law and Cyber Crime

The term 'cyber' is not new as it can be traced back to 1984 when William Gibson first used the term 'cyberspace' in his science fiction novel 'Neuromancer'. The author used the phrase to describe the online world of computers.

For law the concept of the internet was unsettling with one person accessing the website from one location to another accessing it from another. The courts were forced to revisit the question of jurisdiction. As the concept of the internet started spreading, there arose a need to govern the internet known as 'cyberlaw'.

Law is constantly trying to catch up with the changing technology. The increasing use of technological advancement has provided mankind with tremendous opportunities for growth, development and at the same time it has also been serving as a breeding ground for unethical and malicious activities. Such unscrupulous activities are always one step ahead of the mechanism adopted by the law enforcing agencies. In today's world everyone is dependent on the computer which is now used to create, transmit, retrieve and store information. The internet has opened a new era for communication. It is widely used in the commercial as well as utility services. Consequently, cybercrime will not only pose a threat for the commercial world but will also hamper the interest of other communities. Although there is no set definition for cyber crime yet in simple terms it may be described as "Cybercrime is when someone uses computers or the internet to do bad things, like stealing personal information, spreading viruses, hacking into systems, or scamming people. It's like committing crimes, but in the digital world instead of the physical one".

Similarly, the term 'cybersecurity' does not have one rigid definition as well because of its complex nature but, one of the most concise definitions can be "it is a body of technologies,

ISSN: 2582-6433

processes and practices which is designed to protect computer, network, program and data from unauthorized access, disclosure, modification, damage and attack"[1]It denotes both physical security as well as the information stored therein. Information Technology Act, 2000 also provides a similar definition where cyber security means "protecting information, equipment, computer, computer resources, devices, communication device and information stored therein from any unauthorized use, access, modification, disclosure, disruption or destruction.

Rise of Artificial Intelligence (AI)

The earliest substantial work related to artificial intelligence was done in the mid of the 20th century by Alan Mathison Turing a British logician and computer pioneer best known for solving the Enigma code which was employed by the Germans during WWII to transmit coded messages. Alan Turingcreated the Turing test in 1950. He suggested using the Turing test to determine whether a computer (or machine) is capable of thinking intelligently like humans. The initial half of the 20thcentury was familiarised with the concept of artificial intelligence robots all thanks to the "heartless" tin man from Wizard of the Oz, humanoid robot which impersonated Maria in Metropolis and continued with human made, remote controlled transformers who replace humans in dangerous situations to movies depicting warfare between humans and artificial intelligence (I robot, The matrix, The Terminator)

Technology is advancing however law is also catching up. According to John McCarthy who coined the term artificial intelligence (AI) in 1956 describes it as "the science and engineering of making intelligent machines especially intelligent computer programs. It is similar to the task of using computers to understand human intelligence but the difference here is AI does not have to confine itself to methods that are highly biologically observable".[2] Undoubtedly AI has brought enormous benefit to humanity over the last few decades and it is gradually becoming a part of digital services that we use in our day to day life. The government globally is considering the deployment of AI systems and applications to facilitate the identification and prediction of crime more concretely.[3]AI is the next step in the technological evolution with its aim to surpass human

[1]Badruddin and Anis Ahmad (2017), Cyber Security Challenges: Some Reflections on Law and Policy in India, The Haryana Police Journal,Volume 1 No. 1, October.
[2] McCarthy, J. "What Is Artificial Intelligence ?". http://www- formal.stanford.edu/jmc/whatisai.pdf accessed November 2, 2022
[3]Burgess, Matt, "Police built an AI to predict violent crime. It was seriously flawed", WIRED, https://www.wired.co.uk/article/police-violence-prediction-ndasaccessed October 28, 2022.

ISSN: 2582-6433

intelligence, contrary to common perception of sentient machines of killer robot which often crosses our minds when we think of self sufficient thinking machines powered by artificial intelligence. Rather, it also has the potential of transforming military effectiveness by intelligently applying itself in matters of administration as well as decision making. The little area where AI lags is where human brain has the potential to multitask, abstract thinking gained by the eyes of evolution, researchers are faced with such challenges in designing algorithms, which could mimic human like behaviour in machines. While human brain is excellent in non- contextual pattern recognition, machines are always context-dependent and can work mostly on specific problems which revolve around similar pattern as a core feature thus limiting its ability to infer vast amount of information that lay beneath the surface of such patterns which only a human brain has an astonishing ability to comprehend.

Use of Artificial Intelligence (AI) in Cyber Crimes

It is the year 2000, when the world met with extreme uncertainty and fear because of such alleged software and hardware problems.[4] Yet it is a year which has seen the beginning of what we now see as a massive technological development. Today the ease of communication with anyone from anywhere across the globe, the development of self driving cars[5], growth of the internet[6], various entertainment options, all of which once seemed like a farfetched dream to many are now in our present reality.

The significant development of AI like use of facial recognition technologies in the criminal justice realm, use of drones, lethal autonomous weapon system (LAWS) to self driving cars when not properly managed without proper oversight has the potential to be used for disruptive purposes which could harm an individual's rights and freedom. AI and Machine learning (ML) has the capacity to respond to cyberattacks more efficiently but due to its high cost and low

[4]Known as the Y2K bug, where the computer programmers feared that as the year 2000 approached the computer might not be able t interpret the two digit code 00 as 2000 but as 1900. This resulted in fear that activates that were programmed on a daily or yearly basis (interest rate, flight schedule, routine maintenance) could be damages. *Y2K Bug, NAT'L GEOGRAPHIC, http://www.nationalgeoggraphic.org/encyclopedia/Y2K-bug/*

[5]California Department of Motor Vehicles developed an Autonomous Vehicle Tester Program. *Testing of autonomous vehicles,* STATE OF CAL. DEP'T OF MOTOR VEHICLES, https://www.dmv.cagov/portal/dmv/detail/vr/autonomus/testing)

[6]Sensors and actuators embedded in physical object_ from roadways to pacemakers-are linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the Internet. These network churn out huge volumes of data that flow to computers for analysis. When objects can both sense the environment and communicate, they become tools for understanding complexity and responding to it swiftly.
Michael Chui et al., *The Internet of Things,* MCKINSLEY&COMPANY (Mar. 2010), http://www.mvkinsmckinsey.com/industries/high-tech/our-insights/the-internet-of-things

ISSN: 2582-6433

budgets of medium and small scale enterprises, it becomes a little difficult for such entities to improve their cyber security capabilities to ward off such imminent threats.

After the advent of COVID-19, the world noticed a rise in the use of technologies and applications based on AI for their day to day activities like remote work, distance learning, online payments or simply streaming a video on demand. Unfortunately, this situation also led to the rise of crimes where international organisations[7], health sector[8], supply chain companies[9] and individuals were targeted. Through AI cybercriminals have not just found a novel way to leverage their unlawful actives but have also found new opportunities to conduct attacks especially designed to target government, individuals or enterprises. They have witnessed the enormous potential of AI and ML for criminal and disruptive purposes[10] and hence, organised criminal groups are now recruiting skilled hackers to perpetrate their malicious agendas using cyber attacks and conduct criminal actives anywhere in the world.[11]

A) Computer as a criminal Tool

AI has been effectively used for phishing and has been proven successful. One of the most common methods to conduct a phishing activity is by profiling the target and sending spam mails to the target. The concept of profiling is commonly studied in the business industry. It is based on customer's previous buying history which may be instrumental for the attacker. The kind of AI program used for gathering intelligence on the target is embedded in Chabot, as named by the previous researchers.[12] It has also been predicted that this chatbot would be used by the attackers to scam customers.

[7]"WHO reports fivefold increase in cyberattacks, urges vigilance"World Health Organization (WHO)(April 23, 2020), available at: https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

[8]"Cyber Attack Suspected in German Woman's Death",The New York Times, September 18, 2020, available at: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html.

[9]Supply Chain, "Lessons Learned from the Vaccine Supply Chain Attack",available at: https://www.supplychaindigital.com/supply-chain-risk-management/lessons-learned-vaccine-supply-chain-attack

[10]Prakarsh andKhanna R, "Artificial Intelligence and Cybercrime- A curate's Egg", Medium, https://medium.com/the-%C3%B3pinion/artificial-intelligence-and-cybercrime-a-curates-egg-2dbaee833be1accessed accessed October 28, 2022

[11]"The Dark Side of Latin America: Cryptocurrency, Cartels, Carding and the Rise of Cybercrime", INSIGHTS p.6, : https://wow.intsights.com/rs/071-ZWD-900/images/Dark%20Side%20of%20Latin%20America.pdf. See also, "The Next, El Chapo is Coming for your Smartphone", https://www.ozy.com/the-new-and-the-next/the-next-el-chapo-might-strike-your-smartphone-and-bank/273903/.)

[12]J.Kietzmann, J. Paschen, and E. Treen, ''Artificial intelligence in advertising: How marketers can leverage artificial intelligence along the consumer journey,'' J. Advertising Res., vol. 58, no. 3, pp. 263–267, 2018.[47] J. Paschen, M. Wilson, and J. J. Ferreira, ''Collaborative intelligence:How human and artificial intelligence create value along the B2B salesfunnel,'' Bus. Horizons, vol. 63, no. 3, pp. 403–414, May 2020

ISSN: 2582-6433

B) Computer as a criminal Target

AI has the speciality to solve previously unsolved task at a lower cost and labour. There are certain offences where the computer acts as the target, such offences are colloquially known as 'hacking'. Given the ubiquitous presence of computers and dependency on the same, such offences create a potentially serious consequence. Crimes where computer becomes the target of hacker, there is a risk such as theft of intellectual property, blackmailing which is often done on the basis of information gained from computerised files such as medical information, personal history etc, sabotaging the critical operating systems and standalone programs which form an integral part of a critical system such as a nuclear test facility, national power grid etc. In all these crimes, the offender uses the computer either to damage the operating system or obtain any information. Unlawful access to government records and criminal justice is another crime that targets computer directly. 'Techno-vandalism' occurs when there is an unauthorised access to a computer which results in damage to a file, in such a case the damage caused may be intentional or accidental. Another crime which falls under this same category is 'trespass', in this case the intruder looks into the personal files which violates the privacy of the owner. This would be technological equivalent to criminal trespass. In all these offences, the offender uses computer either to obtain information or damage any operating programs.

How Artificial Intelligence (AI) is helping in combating Cyber Crime

AI has now emerged as a dependable alternative to face threats of the cyber world. ML and AI both integrated are now being used to track unlawful and ill-intention activities. AI in security system is frequently used to distinguish between the good and the bad, more advanced system can go beyond this and can analyse large chunk of data and assisting pieces together of connected activities that may signal towards any suspicious behaviour by anonymous entities. AI has the potential to foresee events and provide preventive actions when it comes to cybersecurity furthermore, AI will be able to identify complex assaults, halt them and prevent cyber criminals from any future attempt by establishing their identities and taking action against them.

Artificial Intelligence (AI) and National security

Immense potential has been shown by the Artificial Intelligence in military field in terms of surveillance, cyber security, military logistics, autonomous vehicles and Lethal Autonomous

ISSN: 2582-6433

Weapons System (LAWS). The past decades has witnessed exponential rise in the adoption of AI in both private and public sectors. There are machines which are able to surpass human intelligence, for example, world's number one chess champion, Garry Kasparov was defeated by IBM Deep Blue in the year 1996. However, this involves too many human inputs. There is still a long way to go where systems will be capable enough to perform tasks which would be similar to human level intelligence.

As per The US National Security Commission on AI (NSCAI) "AI will be a source of tremendous power for countries and companies which are ready to harness them"[13] Artificial Intelligence has brought transformation in the domain of hybrid warfare[14] . Proliferation of AI is bringing changes not just in information and economic domain but in military domain as well.[15] Now AI is being widely used for image classification from drone, geospatial data analysis, video and audio analysis as well as deep fakes. AI in today's world with such a vast amount of data pool can provide ample amount of opportunities like:

1. Creation of autonomous and semi autonomous systems: AI systems can collectively increase the geographical reach of the military, for example: autonomous systems can be employed to further increase the border security of the state without endangering the lives of soldiers and can be incorporated in all major military vehicles including fighter aircrafts, naval vessels and ground vehicles. Lethal Autonomous Weapon System (LAWS): they are special class of weapons which use sensors and computer algorithms to independently identify any target and can destroy targets without manual human control.
2. Logistical ability: AI can ensure continuous observation of border and can provide intelligent inputs with regards to need for repairs.
3. Cyber operation: AI can play as a key technology in future military cyber operations both in terms of offensive and defensive capacity.

The global leaders are employing AI in their national security, in the year 2017 China announced their next generation plan with an aim to assume global leadership in AI innovation, Valdimir

[13]Gorman C, **"**Recent Developments in AI and National Security: What You Need to Know**"**, Lawfare, 3 March 2022.
[14]Allen G and Chan T, **"**Artificial Intelligence and National Securit**y"**, BelferCenter for Science and International Affairs, Harvard Kennedy School, 2017.
[15]*Supra*

ISSN: 2582-6433

Putin In 2019 made a statement saying "He who can establish monopoly in artificial intelligence can truly rule the world". These developments highlights the importance that AI is assuming globally, as we are moving ahead it is getting clearer how nation's strength in AI is becoming intertwined to its geopolitical standing. Keeping this in mind it is safe to assume that success in AI has the potential to alter the current balance of power between the nation states.

Use of Artificial Intelligence (AI) in hampering National Security

Russia- Ukraine Conflict:-

Today countries with geopolitical conflicts are using AL and ML in cyberattacks, misinformation campaigns to their advantage, this is apparent from the Russia-Ukraine conflict. Russia has been suspected of using asymmetric warfare by involving in AI based cyberattacks, electronic warfare and information weapons on the other country's infrastructure like electrical gridsand communication systems. Russia previously also has been involved in using discreet mode of technology for destabilising its opponent's infrastructures. Russia is spearheading its AI strategy with heavy investment in its military, state sponsored actors as well as private sector. It is also suspected that with Russia's more and more adoptionin such futuristic technologies and modern battlefield capabilities wit might outmatch US in areas of artillery, armour, air defence, space and cyber space.[16]

AI plays a vital role in the field of information warfare which is evident in the ongoing conflict, as AI helps in analysing vast amount of open source intelligence from videos to telegram posts on troops and attack, one major issue with use of such technology is deep fakes that uses AI techniques to create realistic videos which can further aid in the launch of disinformation campaigns. However, ML can detect such fake videos and hence been used by various social media platforms as well. Russia has heavily used three from information warfare against Ukraine which are:-

1. Disinformation
2. Cyber warfare
3. Kinetic warfare

[16]Peter L. Jones, Ricky Waddell, Wilson Jr C. Blythe and Thomas Pappas, **"**Unclassified Summary of the US Army Training and Doctrine Command Russian New Generation Warfare Study"**,** *TRADOC Ft. Eustis United States*, 2017.)

ISSN: 2582-6433

China growing its AI capacity:-

China has a long history of attacking government organisations, private sector, critical infrastructure and human rights activist in India, it has been going on since 2008 when china was accused of attempting to hack government organisations like the Ministry of External Affairs and National Information Centre,[17] DRDO[18]and so on. India has been a victim of major Chinese espionage operations along with other countries where its civil society, government, and private organisations have been compromised. Keeping in mind the cyber conflict between Russia and Ukraine with use of operations to target critical infrastructure along with cyber espionage, India needs to have a robust strategy to not just detect but to expose china's cyber espionage campaign. What India needs right now, is to reinforce intelligence gathering and enhance collaboration with private tech companies that have the required expertise.

Conclusion:

With proliferation of AI, the weapons of wars are now becoming more and more technologically equipped, which in turn is changing the battlefield scenarios The anonymity with the use of AI based asymmetric warfare like information warfare and cyber warfare allows countries to flex their power, Furthermore this makes the impact more offensive by destabilising any country without any geographical restrictions causing direct and more severe impact on the economy of the country. AI will be the future of war, since it plays a significant role in developing advanced autonomous system, any country with indigenous development of such system will lead the battlefield as the inconspicuous use of technology will the first step to disable the opponent's infrastructure. AI has enormous benefit in both military and civil uses but it is essential for countries to invest more in such technological advancement in order to protect itself not just from cyber threat but from security threat as well.

[17]Indrani Bagchi, **"**China Mounts Cyber Attacks On Indian Sites", *The Times of India*, 5 May 2008.) PM's Office in 2010 (Ashish Khetan, **"**Chinese Hackers Target PMO**"**, *India Today*, 14 January 2010.
[18]Mohit Kumar, **"**Chinese Hackers Infiltrate Indian Defence Research Organisation**"**, *The Hacker News*, 13 March 2013.